

Class Numbers of Orders in Quartic Fields

Anton Deitmar & Mark Pavey

Introduction

Let \mathcal{D} be the set of all natural numbers $D \equiv 0, 1 \pmod{4}$ with D not a square. Then \mathcal{D} is the set of all discriminants of orders in real quadratic fields. For $D \in \mathcal{D}$ the set

$$\mathcal{O}_D = \left\{ \frac{x + y\sqrt{D}}{2} : x \equiv yD \pmod{2} \right\}$$

is an order in the real quadratic field $\mathbb{Q}(\sqrt{D})$ with discriminant D . As D varies, \mathcal{O}_D runs through the set of all orders of real quadratic fields. For $D \in \mathcal{D}$ let $h(\mathcal{O}_D)$ denote the class number and $R(\mathcal{O}_D)$ the regulator of the order \mathcal{O}_D . It was conjectured by Gauss ([15]) and proved by Siegel ([34]) that, as x tends to infinity

$$\sum_{\substack{D \in \mathcal{D} \\ D \leq x}} h(\mathcal{O}_D) R(\mathcal{O}_D) = \frac{\pi^2 x^{3/2}}{18\zeta(3)} + O(x \log x),$$

where ζ is the Riemann zeta function.

For a long time it was believed to be impossible to separate the class number and the regulator in the summation. However, in [32], Theorem 3.1, Sarnak showed, using the Selberg trace formula, that as $x \rightarrow \infty$ we have

$$\sum_{\substack{D \in \mathcal{D} \\ R(\mathcal{O}_D) \leq x}} h(\mathcal{O}_D) \sim \frac{e^{2x}}{2x}.$$

More sharply,

$$\sum_{\substack{D \in \mathcal{D} \\ R(\mathcal{O}_D) \leq x}} h(\mathcal{O}_D) = L(2x) + O\left(e^{3x/2} x^2\right)$$

as $x \rightarrow \infty$, where $L(x)$ is the function $L(x) = \int_1^x \frac{e^t}{t} dt$. Sarnak established this result by identifying the regulators with lengths of closed geodesics of the modular curve $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$, where \mathbb{H} denotes the upper half-plane, and using the Prime Geodesic Theorem for this Riemannian surface. Actually Sarnak proved not this result but the analogue where $h(\mathcal{O})$ is replaced by the class number in the narrower sense and $R(\mathcal{O})$ by a “regulator in the narrower sense”. But in Sarnak’s proof the group $\mathrm{SL}_2(\mathbb{Z})$ can be replaced by $\mathrm{PGL}_2(\mathbb{Z})$ giving the above result.

The Prime Geodesic Theorem in this context gives an asymptotic formula for the number of closed geodesics on the surface $\mathrm{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ with length less than or equal to $x > 0$. This formula is analogous to the asymptotic formula for the number of primes less than x given in the Prime Number Theorem. The Selberg zeta function (see [33]) is used in the proof of the Prime Geodesic Theorem in a way analogous to the way the Riemann zeta function is used in the proof of the Prime Number Theorem (see [5]). The required properties of the Selberg zeta function are deduced from the Selberg trace formula ([33]).

It seems that following Sarnak’s result no asymptotic results for class numbers in fields of degree greater than two were proven until in [9], Theorem 1.1, the first named author proved an asymptotic formula for class numbers of orders in complex cubic fields, that is, cubic fields with one real embedding and one pair of complex conjugate embeddings. This result can be stated as follows.

Let S be a finite set of prime numbers containing at least two elements and let $C(S)$ be the set of all complex cubic fields F such that all primes $p \in S$ are non-decomposed in F . For $F \in C(S)$ let $\mathcal{O}_F(S)$ be the set of all isomorphism classes of orders in F which are maximal at all $p \in S$, ie. are such that the completion $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$ is the maximal order of the field $F_p = F \otimes \mathbb{Q}_p$ for all $p \in S$. Let $O(S)$ be the union of all $\mathcal{O}_F(S)$, where F ranges over $C(S)$. For a field $F \in C(S)$ and an order $\mathcal{O} \in \mathcal{O}_F(S)$ define

$$\lambda_S(\mathcal{O}) = \lambda_S(F) = \prod_{p \in S} f_p(F),$$

where $f_p(F)$ is the inertia degree of p in F . Let $R(\mathcal{O})$ denote the regulator and $h(\mathcal{O})$ the class number of the order \mathcal{O} .

For $x > 0$ we define

$$\pi_S(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}(S) \\ R(\mathcal{O}) \leq x}} \lambda_S(\mathcal{O}) h(\mathcal{O}).$$

Then as $x \rightarrow \infty$ we have

$$\pi_S(x) \sim \frac{e^{3x}}{3x}.$$

More sharply,

$$\pi_S(x) = L(3x) + O\left(\frac{e^{9x/4}}{x}\right)$$

as $x \rightarrow \infty$.

This result was again proved by means of a Prime Geodesic Theorem, this time for symmetric spaces formed as a compact quotient of the group $\mathrm{SL}_3(\mathbb{R})$. There exists a Selberg trace formula for such spaces ([36]) by means of which the required properties of a generalised Selberg zeta function can be deduced ([8]) in order to prove the Prime Geodesic Theorem. The class number formula is then deduced by means of a correspondence between primitive closed geodesics and orders in complex cubic number fields, under which the lengths of the geodesics correspond to the regulators of the number fields.

In this paper we follow the methods of [9]. We make use of the prime geodesic theorem in [13]. Let us quote this result as follows.

Let $G = \mathrm{SL}_4(\mathbb{R})$ and let K be the maximal compact subgroup $\mathrm{SO}(4)$. Let $\Gamma \subset G$ be discrete and cocompact. We then have a one to one correspondence between conjugacy classes in Γ and free homotopy classes of closed geodesics on the symmetric space $X_\Gamma = \Gamma \backslash G/K$. Let

$$A^- = \left\{ \begin{pmatrix} a & & & \\ & a & & \\ & & a^{-1} & \\ & & & a^{-1} \end{pmatrix} : 0 < a < 1 \right\}$$

and

$$B = \begin{pmatrix} \mathrm{SO}(2) & \\ & \mathrm{SO}(2) \end{pmatrix}.$$

Let $\mathcal{E}(\Gamma)$ be the set of primitive conjugacy classes $[\gamma]$ in Γ such that γ is conjugate in G to an element $a_\gamma b_\gamma$ of $A^- B$. For $\gamma \in \Gamma$ we write a_γ also for the top left entry in the matrix a_γ and define the length l_γ of γ to be $8 \log a_\gamma$. Let G_γ, Γ_γ be the centralisers of γ in G and Γ respectively and let $K_\gamma = K \cap G_\gamma$. For $x > 0$ define the function

$$\pi(x) = \sum_{\substack{[\gamma] \in \mathcal{E}(\Gamma) \\ e^{l_\gamma} \leq x}} \chi_1(\Gamma_\gamma),$$

where $\chi_1(\Gamma_\gamma)$ is the first higher Euler characteristic of the symmetric space $X_{\Gamma_\gamma} = \Gamma_\gamma \backslash G_\gamma / K_\gamma$.

Theorem 0.1 (Prime Geodesic Theorem) *For $x \rightarrow \infty$ we have*

$$\pi(x) \sim \frac{2x}{\log x}.$$

More sharply,

$$\pi(x) = 2 \mathrm{li}(x) + O\left(\frac{x^{3/4}}{\log x}\right)$$

as $x \rightarrow \infty$, where $\mathrm{li}(x) = \int_2^x \frac{1}{\log t} dt$ is the integral logarithm.

We now state our result on class numbers. Let S be a finite, non-empty set of prime numbers containing an even number of elements. We define the sets $C(S)$ and $O(S)$ and the constants $\lambda_S(\mathcal{O})$ as above, replacing complex cubic fields with totally complex quartic fields in the definitions. A totally complex quartic field has at most one real quadratic subfield, as can be seen by comparing numbers of fundamental units. Let $C^c(S) \subset C(S)$ be the subset of fields with no real quadratic subfield and let $O^c(S) \subset O(S)$ be the subset of isomorphism classes of orders in fields in $C^c(S)$. Let $R(\mathcal{O})$ and $h(\mathcal{O})$ once again denote respectively the regulator and class number.

Theorem 0.2 (Main Theorem) *For $x > 0$ we define*

$$\pi_S(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S) \\ R(\mathcal{O}) \leq x}} \lambda_S(\mathcal{O}) h(\mathcal{O}).$$

Then as $x \rightarrow \infty$ we have

$$\pi_S(x) \sim \frac{e^{4x}}{8x}.$$

Note the surprising factor $1/2!$ We give an explanation below.

Transferring the methods of [9] to the case of totally complex quartic fields does not proceed entirely smoothly, there are various technical difficulties to be overcome. For instance, the correspondence between primitive closed geodesics and orders is considerably more complicated than in either the real quadratic or the complex cubic case. As a result of this extra complexity our result is weaker than that obtained in the complex cubic case. We have had to impose the extra condition on the finite set S of prime numbers that it must contain an even number of elements and we have been unable to provide an error term in our final asymptotic.

Also we have had to restrict ourselves to counting the orders in fields without a real quadratic subfield, as the fields with a real quadratic subfield cannot be counted using our method. Indeed, any real quadratic field which occurs as a subfield of a totally complex quartic field may in fact occur as a subfield of infinitely many such fields. The fundamental units in the quadratic field are powers of fundamental units in the quartic fields, so the (possibly infinitely many) quartic fields all have regulator less than or equal to that of the quadratic field. Hence an asymptotic formula for a sum of class numbers of orders bounded by the regulators is not even possible in the case of totally complex quartic fields with a real subfield.

In comparison with the real quadratic and complex cubic cases one might have expected to get the asymptotic $\pi_S(x) \sim \frac{e^{4x}}{4x}$. In the result that we do in fact get there is an extra factor of one half. The fact that we have had to restrict the fields over which we are counting gives an explanation for this discrepancy.

We also prove the following asymptotic in which we introduce an extra factor into the summands. For an order $\mathcal{O} \in \mathcal{O}(S)$ this extra factor is defined in terms of the arguments of the fundamental units of \mathcal{O} under the embeddings of F into \mathbb{C} as follows. If ε is a fundamental unit in \mathcal{O} then $\varepsilon^{-1}, \zeta\varepsilon$ and $\zeta\varepsilon^{-1}$ are also fundamental units in \mathcal{O} , where ζ is a root of unity contained in \mathcal{O} . Let

$$\nu(\mathcal{O}) = \frac{1}{2\mu_{\mathcal{O}}} \sum_{\varepsilon} \prod_{\alpha} \left(1 - \frac{\alpha(\varepsilon)}{|\alpha(\varepsilon)|} \right),$$

where $\mu_{\mathcal{O}}$ is the number of roots of unity in \mathcal{O} , the sum is over the $2\mu_{\mathcal{O}}$ different fundamental units of \mathcal{O} and the product is over the embeddings of \mathcal{O} into \mathbb{C} . We have:

Theorem 0.3 *For $x > 0$ we define*

$$\tilde{\pi}_S(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S) \\ R(\mathcal{O}) \leq x}} \nu(\mathcal{O}) \lambda_S(\mathcal{O}) h(\mathcal{O}).$$

Then as $x \rightarrow \infty$ we have

$$\tilde{\pi}_S(x) \sim \frac{e^{4x}}{2x}.$$

An element γ in Γ is called *regular* if it centraliser in G is a torus and *non-regular* otherwise. The factor $\nu(\mathcal{O})$ was originally introduced in order to separate the contribution of non-regular elements from that of the regular elements in the Prime Geodesic Theorem. As it turned out, the complexity of the correspondence between geodesics and orders meant that we did not really gain anything from this approach. However, the factor $\nu(\mathcal{O})$ contains information about the arguments of the fundamental units in the order \mathcal{O} which is interesting in its own right. In comparison with Theorem 0.2 we can see that “on average” the value of $\nu(\mathcal{O})$ as $R(\mathcal{O})$ goes to infinity is 4. If ε is a fundamental unit in \mathcal{O} with arguments $\theta, -\theta, \phi, -\phi$ under the four embeddings of \mathcal{O} into \mathbb{C} then a simple calculation shows that

$$\prod_{\alpha} \left(1 - \frac{\alpha(\varepsilon)}{|\alpha(\varepsilon)|} \right) = 4(1 - \cos 2\theta)(1 - \cos 2\phi).$$

Since this takes “on average” the value 4 we can see that there is a sense in which we can say that the arguments of the fundamental units in the orders \mathcal{O} are evenly distributed about $\pm\pi/2$ as $R(\mathcal{O})$ goes to infinity.

In what follows we give a summary of the arguments and techniques used in the proof of our main results. In particular we shall point out the difficulties that arise in applying the methods of [9] to our situation.

In Section 1 we use a classification of the set of equivalence classes of division algebras over \mathbb{Q} by means of a description of the Brauer group of \mathbb{Q} ([28], Theorem 18.5) to show the existence of a division algebra $M(\mathbb{Q})$ whose maximal subfields include the fields in the set $C^c(S)$ and such that $M(\mathbb{Q}) \otimes \mathbb{R} \cong \text{Mat}_4(\mathbb{R})$. In fact the maximal subfields of $M(\mathbb{Q})$ are all quartic extensions of \mathbb{Q} and the set of totally complex maximal subfields of $M(\mathbb{Q})$ coincides with $C(S)$. We further show that for an order \mathcal{O} in $O(S)$ the number of embeddings of \mathcal{O} into $M(\mathbb{Q})$, up to conjugation by the unit group of the maximal order $M(\mathbb{Z})$, is $\lambda_S(\mathcal{O})h(\mathcal{O})$. The restriction on the set S of prime numbers that it has to contain an even number of elements is a consequence of the classification of division algebras over \mathbb{Q} .

In Section 2 we prove a correspondence between the primitive, closed geodesics in the Prime Geodesic Theorem and the orders of totally complex quartic fields. Under this correspondence the lengths of the geodesics correspond to the regulators of the orders. It turns out that it is the regular, weakly neat elements of $\mathcal{E}(\Gamma)$ which correspond to orders in totally complex quartic fields with no real quadratic subfield. We use a “sandwiching” argument to isolate these elements in the Prime Geodesic Theorem.

We finish this introduction with a few remarks about the limitations of the method used here in terms of further applications and mention a couple of other recent results in the same direction. In order to be able to make use of the trace formula for compact spaces we have had to limit our sum over class numbers by means of the choice of a finite set of primes, as described above. In [12] Deitmar and Hoffmann have been able to use a different trace formula to prove that as $x \rightarrow \infty$

$$\sum_{R(\mathcal{O}) \leq x} h(\mathcal{O}) \sim \frac{e^{3x}}{3x},$$

where the sum is over all isomorphism classes of orders in complex cubic fields.

In order to get the error term in the Prime Geodesic Theorem we have made use of the classification of the unitary dual of $\text{SL}_4(\mathbb{R})$. At present the unitary dual is not known for any higher dimensional groups so a Prime Geodesic Theorem with error term is not possible using our methods. Finally we mention that the correspondence between geodesics and orders actually works by identifying primitive geodesics with fundamental units in orders. By Dirichlet’s unit theorem, an order in a number field F has a unique fundamental unit (up to inversion and multiplication by a root of unity) only if F is real quadratic, complex cubic or totally complex quartic. Hence an asymptotic of our form can be proven only in these three cases. In [10], the first named author has proved a Prime Geodesic Theorem for higher rank spaces, from which he deduces an asymptotic formula for class numbers of orders in totally real number fields of prime degree.

1 Division Algebras of Degree Four

1.1 Central simple algebras and orders

Let F be a field. Let $\mathcal{C}(F)$ denote the set of isomorphism classes of finite dimensional central simple algebras over F and $\mathcal{D}(F)$ the set of isomorphism classes of finite dimensional division algebras with centre F , then $\mathcal{D}(F) \subset \mathcal{C}(F)$.

For convenience we collect together here a number of facts about central simple algebras and their orders, which will be used in the sequel. Let F be a field, K an extension of F and A a finite dimensional algebra over F .

Proposition 1.1 (a) If $n = \dim_F A$, then there exists an injective homomorphism $A \hookrightarrow \text{Mat}_n(F)$.

(b) $\dim_K(A \otimes K) = \dim_F A$.

(c) If $A \in \mathcal{C}(F)$, then $A \otimes K \in \mathcal{C}(K)$.

(d) If B is a simple subalgebra of $A \in \mathcal{C}(F)$ with centraliser $C_A(B)$ in A , then

$$(\dim_F B)(\dim_F C_A(B)) = \dim_F A.$$

Proof: All the statements of the proposition are proved in [28]. Statement (a) is Corollary 5.5b; (b) is Lemma 9.4; (c) is Proposition 12.4b(ii) and (d) is Theorem 12.7. \square

The next proposition gives some results about subfields of algebras.

Proposition 1.2 (a) If $A \in \mathcal{D}(F)$, then for every $x \in A$ the set $F[x] = \{f(x) : f \in F[X]\}$ is a subfield of A .

(b) If $A \in \mathcal{C}(F)$, then $\dim_F A = m^2$ for some $m \in \mathbb{N}$. The natural number m is called the degree of A . If E is a subfield of A then $[E : F]$ divides m .

If K is a subfield of A containing F then it is said to be strictly maximal if $[K : F] = \deg A$.

(c) A subfield K of $A \in \mathcal{C}(F)$ is strictly maximal if and only if $C_A(K) = K$. If $A \in \mathcal{D}(F)$ then every maximal subfield of A is strictly maximal.

(d) If $A \in \mathcal{C}(F)$ and $[K : F] = \deg A = n$, then $A \otimes K \cong \text{Mat}_n(K)$ if and only if K is isomorphic as an F -algebra to a strictly maximal subfield of A .

Proof: All the statements of the proposition are proved in [28]. Statement (a) is Lemma 13.1b; (b) is Corollary 13.1a; (c) is Corollary 13.1b and (d) is Corollary 13.3. \square

Now let F be a number field and \mathcal{O}_F the ring of integers in F . For any finite dimensional vector space V over F , a full \mathcal{O}_F -lattice in V is a finitely generated \mathcal{O}_F -submodule M in V which contains a basis of V . A subring \mathcal{O} of A which is also a full \mathcal{O}_F -lattice in A is called an \mathcal{O}_F -order, or simply an order, in A . A maximal \mathcal{O}_F -order in A is an \mathcal{O}_F -order which is not properly contained in any other \mathcal{O}_F -order in A . An element $a \in A$ is said to be integral over \mathcal{O}_F if it is a root of a monic polynomial with coefficients in \mathcal{O}_F . The integral closure of \mathcal{O}_F in A is the set of all elements of A which are integral over \mathcal{O}_F .

Proposition 1.3 (a) (Skolem-Noether Theorem) Let $A \in \mathcal{C}(F)$, and B a simple subring of A such that $F \subset B \subset A$. Then every F -isomorphism of B onto a subalgebra of A extends to an inner automorphism of A .

(b) Every element of an \mathcal{O}_F -order \mathcal{O} is integral in A over \mathcal{O}_F .

(c) The \mathcal{O}_F -order \mathcal{O} is maximal in A if and only if for each prime ideal \mathfrak{p} of \mathcal{O}_F the \mathfrak{p} -adic completion $\mathcal{O}_{\mathfrak{p}}$ is a maximal $\mathcal{O}_{F,\mathfrak{p}}$ -order in $A_{\mathfrak{p}}$.

(d) If $A \in \mathcal{D}(F_{\mathfrak{p}})$ for some prime ideal \mathfrak{p} of \mathcal{O}_F , then the integral closure of $\mathcal{O}_{F,\mathfrak{p}}$ in A is the unique maximal $\mathcal{O}_{F,\mathfrak{p}}$ -order in A .

Proof: All the statements of the proposition are proved in [31]. Statement (a) is Theorem 7.21; (b) is Theorem 8.6; (c) is Corollary 11.6 and (d) is Theorem 12.8. \square

1.2 Division algebras of degree four

Let A be a central simple algebra over a field F . By the Wedderburn Structure Theorem ([28], Theorem 3.5) the algebra A is isomorphic to $\text{Mat}_n(D)$, where $n \in \mathbb{N}$ and D is a finite dimensional division algebra over F , which by [28], Proposition 12.5b is unique up to isomorphism. If B is another central simple algebra over F isomorphic to $\text{Mat}_m(E)$, where $m \in \mathbb{N}$ and E is a finite dimensional division algebra over

F , then A and B are called *Morita equivalent* if and only if $D \cong E$. By [28], Proposition 12.5a, the tensor product over F induces a group structure on the set of equivalence classes. The group defined in this way is called the *Brauer group*.

By [28], Theorem 17.10, if F is a local, non-archimedean field, then there is a canonical isomorphism between the Brauer group of F and the group \mathbb{Q}/\mathbb{Z} . The *Brauer invariant* $\text{Inv } A$ of A is defined to be the image in \mathbb{Q}/\mathbb{Z} of the Morita equivalence class of A under this isomorphism. The *Schur index* $\text{Ind } A$ of A is defined to be the degree of D . By [28], Corollary 17.10a(iii), the order of the Brauer invariant of A in \mathbb{Q}/\mathbb{Z} equals $\text{Ind } A$.

The only (associative) division algebras over \mathbb{R} are \mathbb{R} itself, \mathbb{C} and the quaternions \mathbb{H} (see [28], Corollary 13.1c). Since \mathbb{C} is itself a field, any algebra which is central simple over \mathbb{R} cannot be isomorphic to a matrix algebra over \mathbb{C} . The Brauer group of \mathbb{R} is therefore isomorphic to $\mathbb{Z}/2\mathbb{Z}$. Let A be a central simple algebra over \mathbb{R} . If $A \cong \text{Mat}_n(\mathbb{R})$ for some $n \in \mathbb{N}$, then the Brauer invariant of A is defined to be zero and the Schur index of A is defined to be one. If $A \cong \text{Mat}_n(\mathbb{H})$ for some $n \in \mathbb{N}$, then the Brauer invariant of A is one half and the Schur index of A is two.

Let M be a division algebra of degree 4 over \mathbb{Q} . Fix a maximal order $M(\mathbb{Z})$ in M . If R is a commutative ring with unit then we denote by $M(R)$ the R -algebra $M(\mathbb{Z}) \otimes_{\mathbb{Z}} R$. In particular we have $M \cong M(\mathbb{Q})$. For any ring R the reduced norm induces a map $\det : M(R) \rightarrow R$. (We note that in the case that $M(R) \cong \text{Mat}_4(R)$ the reduced norm of an element of $M(R)$ equals its determinant, justifying the choice of notation; see [28], Chapter 16.)

Let p be a prime. From Proposition 1.1(b) we know that $\deg M(\mathbb{Q}_p) = \deg M(\mathbb{Q}) = 4$. It then follows that if $\text{Inv } M(\mathbb{Q}_p)$ is equal to $\frac{1}{4}$ or $\frac{3}{4}$ then $M(\mathbb{Q}_p)$ is a division algebra of degree four over \mathbb{Q}_p , and if $\text{Inv } M(\mathbb{Q}_p) = 0$ then $M(\mathbb{Q}_p) \cong \text{Mat}_4(\mathbb{Q}_p)$. The other possibility, that $\text{Inv } M(\mathbb{Q}_p) = \frac{1}{2}$, does not interest us here. Proposition 1.1(b) also tells us that $\deg M(\mathbb{R}) = 4$. We know that $\text{Inv } M(\mathbb{R})$ equals zero or one half. It follows that $M(\mathbb{R})$ is isomorphic to $\text{Mat}_4(\mathbb{R})$ or $\text{Mat}_2(\mathbb{H})$ respectively.

Let S be a finite, non-empty set of prime numbers with an even number of elements. We say that $M(\mathbb{Q})$ *splits* over a prime p if $M(\mathbb{Q}_p) \cong \text{Mat}_4(\mathbb{Q}_p)$. For all primes p we define i_p as follows. If $p \in S$ define i_p to be either $\frac{1}{4}$ or $\frac{3}{4}$ in such a way that $\sum_{p \in S} i_p \in \mathbb{Z}$. Note that we are able to do this since we have specified that S must contain an even number of elements. For all other p define $i_p = 0$. Then [28], Theorem 18.5 tells us that we may choose M so that $\text{Inv } M(\mathbb{Q}_p) = i_p$ for all primes p and $\text{Inv } M(\mathbb{R}) = 0$. We can then see that the set of places at which $M(\mathbb{Q})$ does not split coincides with the set S . More particularly, for $p \in S$ we have that $M(\mathbb{Q}_p)$ is a division \mathbb{Q}_p -algebra, for $p \notin S$ we have that $M(\mathbb{Q}_p) \cong \text{Mat}_4(\mathbb{Q}_p)$ and we also have $M(\mathbb{R}) \cong \text{Mat}_4(\mathbb{R})$.

For a commutative ring R with unity, let

$$\mathcal{G}(R) = \{x \in M(R) : \det(x) = 1\}.$$

Then \mathcal{G} is a linear algebraic group, defined over \mathbb{Z} . Let $\Gamma = \mathcal{G}(\mathbb{Z})$, then Γ forms a discrete subgroup of $G = \mathcal{G}(\mathbb{R}) \cong \text{SL}_4(\mathbb{R})$. Since $M(\mathbb{Q})$ is a division algebra, it follows that \mathcal{G} is anisotropic over \mathbb{Q} and so Γ is cocompact in G (see [2], Theorem A). Let P be the parabolic subgroup

$$P = \begin{pmatrix} * & * \\ 0 & 0 & * \\ 0 & 0 \end{pmatrix}$$

of G . Then $P = MAN$, where

$$\begin{aligned} M &= S \begin{pmatrix} \text{SL}_2^{\pm}(\mathbb{R}) & \\ & \text{SL}_2^{\pm}(\mathbb{R}) \end{pmatrix} \\ &= \left\{ \begin{pmatrix} X & \\ & Y \end{pmatrix} : X, Y \in \text{Mat}_2(\mathbb{R}), \det X = \det Y = \pm 1 \right\}, \end{aligned}$$

$A = \{\text{diag}(a, a, a^{-1}, a^{-1}) : a > 0\}$ and the elements of N have ones on the diagonal and the only other non-zero entries in the top right two by two square. Let

$$B = \begin{pmatrix} \text{SO}(2) & \\ & \text{SO}(2) \end{pmatrix}.$$

Then B is a compact subgroup of M .

Let $A^- = \{\text{diag}(a, a, a^{-1}, a^{-1}) : a \in (0, 1)\}$ be the negative Weyl chamber of A . Let $\mathcal{E}_P(\Gamma)$ be the set of conjugacy classes $[\gamma]$ in Γ such that γ is conjugate in G to an element $a_{\gamma} b_{\gamma}$ of $A^- B$ and let $\mathcal{E}_P^p(\Gamma)$ be the subset of primitive conjugacy classes.

We say $g \in G$ is *regular* if its centraliser is a torus and *non-regular* (or *singular*) otherwise. Clearly, for $\gamma \in \Gamma$ regularity is a property of the Γ -conjugacy class $[\gamma]$, we denote by $\mathcal{E}_P^{p,\text{reg}}(\Gamma)$ the regular elements of $\mathcal{E}_P^p(\Gamma)$. By abuse of notation we sometimes write $\gamma \in \mathcal{E}_P^p(\Gamma)$ or $\gamma \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$ when we mean the conjugacy class of γ .

We will call a quartic field extension F/\mathbb{Q} *totally complex* if it has two pairs of conjugate complex embeddings and no real embeddings into \mathbb{C} .

1.3 Subfields of $M(\mathbb{Q})$ generated by Γ

Lemma 1.4 *Let $[\gamma] \in \mathcal{E}_P(\Gamma)$.*

The centraliser $M(\mathbb{Q})_\gamma$ of γ in $M(\mathbb{Q})$ is a totally complex quartic field if and only if γ is regular.

The centraliser $M(\mathbb{Q})_\gamma$ is a quaternion algebra over the real quadratic field $\mathbb{Q}[\gamma]$ if and only if γ is non-regular.

Proof: The centraliser $M(\mathbb{Q})_\gamma$ of γ in $M(\mathbb{Q})$ is a division subalgebra of $M(\mathbb{Q})$. Suppose that $M(\mathbb{Q})_\gamma = \mathbb{Q}$. Then since $\gamma \in M(\mathbb{Q})_\gamma$ we must have $\gamma \in \mathbb{Q}$, but then γ is central so $M(\mathbb{Q})_\gamma = M(\mathbb{Q})$, a contradiction. Suppose instead that $M(\mathbb{Q})_\gamma = M(\mathbb{Q})$, ie. γ is central. Then $\gamma \in \mathbb{Q}$, so $\det \gamma = \gamma^4 = 1$ and it follows that $\gamma = \pm 1$, which possibility is excluded since $\gamma = \pm 1$ is not primitive.

By Proposition 1.1(d) we have that $\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma$ divides $\dim_{\mathbb{Q}} M(\mathbb{Q})$, which is 16, so $\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma$ is equal to 2, 4 or 8. Also

$$\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma = \dim_{\mathbb{R}} M(\mathbb{R})_\gamma = \dim_{\mathbb{R}} M(\mathbb{R})_{a_\gamma b_\gamma}.$$

Depending on whether neither, one or both of the $\text{SO}(2)$ components of b_γ are $\pm I_2$, the dimension $\dim_{\mathbb{R}} M(\mathbb{R})_{a_\gamma b_\gamma}$ is equal to 4, 6 or 8 respectively. Hence $\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma$ is either 4 or 8. If $\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma = 4$ then $b_\gamma = (R(\theta), R(\phi))$ with $\theta, \phi \notin \pi\mathbb{Z}$, where

$$R(\theta) = \begin{pmatrix} \cos \theta & -\sin \theta \\ \sin \theta & \cos \theta \end{pmatrix}.$$

If $\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma = 8$ then b_γ is diagonal.

In the first case $G_\gamma \cong AB \cong \mathbb{R}^+ \times \text{SO}(2) \times \text{SO}(2)$ so γ is regular. From Proposition 1.1(d) and Proposition 1.2(a) it follows that $\mathbb{Q}[\gamma]$ is a subfield of $M(\mathbb{Q})$ of degree 4. Let $f_\gamma(x)$ be the minimal polynomial of γ over \mathbb{Q} . Then $a_\gamma b_\gamma$ also satisfies $f_\gamma(x) = 0$. Now $a_\gamma = \text{diag}(a, a, a^{-1}, a^{-1})$ for some $a \in (0, 1)$ and $b_\gamma = (R(\theta), R(\phi))$ for some $\theta, \phi \notin \pi\mathbb{Z}$, so the complex numbers $z_1 = ae^{i\theta}$ and $z_2 = a^{-1}e^{i\phi}$ also satisfy $f_\gamma(x) = 0$. Neither z_1 nor z_2 are real, nor do we have $z_1 = \bar{z}_2$, so $\mathbb{Q}[\gamma] \cong \mathbb{Q}[z_1, z_2]$, which is a totally complex field. The division subalgebra $M(\mathbb{Q})_\gamma$ of $M(\mathbb{Q})$ has dimension four over \mathbb{Q} and contains $\mathbb{Q}[\gamma]$, hence is equal to $\mathbb{Q}[\gamma]$.

Suppose instead that b_γ is diagonal. Then $G_\gamma \cong AM$, so γ is not regular. From Proposition 1.1(d) and Proposition 1.2 (a) it follows that $\mathbb{Q}[\gamma] = \{f(\gamma) : f(x) \in \mathbb{Q}[x]\}$ is a subfield of $M(\mathbb{Q})$ of degree 2. Let $f_\gamma(x)$ be the minimal polynomial of γ over \mathbb{Q} . Then $a_\gamma b_\gamma$ also satisfies $f_\gamma(x) = 0$. Now $a_\gamma = \text{diag}(a, a, a^{-1}, a^{-1})$ for some $a \in (0, 1)$ and $b_\gamma = (\pm I_2, \pm I_2)$. Let us suppose that $b_\gamma = I_4$, the other cases are similar. Then $f_\gamma(a) = f_\gamma(a^{-1}) = 0$, so $f_\gamma = (x - a)(x - a^{-1})$ and $\mathbb{Q}[\gamma]$ is a real quadratic field.

The division algebra $M(\mathbb{Q})_\gamma$ is central simple over its centre $Z(M(\mathbb{Q})_\gamma)$. Clearly, $\mathbb{Q}[\gamma]$ is contained in $Z(M(\mathbb{Q})_\gamma)$. By Proposition 1.2(b), the dimension of $M(\mathbb{Q})_\gamma$ over its centre is m^2 for some $m \in \mathbb{N}$. Hence either $M(\mathbb{Q})_\gamma$ is a field or $Z(M(\mathbb{Q})_\gamma) = \mathbb{Q}[\gamma]$. However, by Proposition 1.2(b) again, if F is a subfield of $M(\mathbb{Q})$ then $[F : \mathbb{Q}] = 1, 2$ or 4 . This rules out the possibility of $M(\mathbb{Q})_\gamma$ being a field, since $\dim_{\mathbb{Q}} M(\mathbb{Q})_\gamma = 8$. We conclude that $Z(M(\mathbb{Q})_\gamma) = \mathbb{Q}[\gamma]$ and by [28], Theorem 13.1, $M(\mathbb{Q})_\gamma$ is a quaternion algebra over $\mathbb{Q}[\gamma]$. \square

1.4 Field and order embeddings

In this section we prove a number of lemmas which will be needed later.

Lemma 1.5 *Let $u \in M(\mathbb{Z})$. Then u is a unit in $M(\mathbb{Z})$ iff $\det(u) = \pm 1$. If $\mathbb{Q}[u]$ is quadratic or is totally complex quartic, or if $u = \pm 1$, then $\det(u) = 1$.*

Proof: By Proposition 1.2(a) the set $F = \mathbb{Q}[u]$ is a subfield of $M(\mathbb{Q})$ containing u . The set $F \cap M(\mathbb{Z})$ is an order in F . The element u is in $F \cap M(\mathbb{Z})$ so by Proposition 1.3(b) it is in the integral closure \mathcal{O}_F of \mathbb{Z} in F .

The field norm $N_{F|\mathbb{Q}} : F \rightarrow \mathbb{Q}$ can be written as a product over all embeddings of F into the complex field, $N_{F|\mathbb{Q}}(x) = \prod_{\sigma} \sigma x$, and it is standard that u is a unit in \mathcal{O}_F if and only if $N_{F|\mathbb{Q}}(u) = \pm 1$. Proposition 16.2a of [28] tells us that

$$\det(u) = N_{F|\mathbb{Q}}(u)^k, \quad (1)$$

where $\deg M(\mathbb{Q}) = k[F : \mathbb{Q}]$. The first statement of the lemma follows.

If $u = \pm 1$ (so that $F = \mathbb{Q}$) or F is quadratic then by (1) we have $\det(u) = 1$. Suppose F is a totally complex quartic extension. Let $f(X) = X^4 + a_3X^3 + a_2X^2 + a_1X + a_0$ be the minimal polynomial of u over \mathbb{Q} . Then $\det(u) = a_0$. If $a_0 = \det(u) = -1$ then f must have a real root, which contradicts the supposition on F . Hence $\det(u) = 1$. \square

The following lemma holds for any algebraic extension F of \mathbb{Q} .

Lemma 1.6 *Let \mathcal{O} be an order in the number field F/\mathbb{Q} and p a prime number. Let $F_p = F \otimes \mathbb{Q}_p$ and $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$. Then \mathcal{O}_p is the maximal order of F_p for all but finitely many primes p .*

Proof: Let \mathcal{O}_M be the maximal order of F and let $\mathcal{O}_{M,p} = \mathcal{O}_M \otimes \mathbb{Z}_p$. We define the *conductor* of \mathcal{O} to be the ideal $\mathfrak{F} = \{\alpha \in \mathcal{O}_M \mid \alpha \mathcal{O}_M \subset \mathcal{O}\}$ of \mathcal{O}_M . Then for all primes p , if $\mathfrak{F} \not\subset p\mathcal{O}_M$, then $\mathcal{O}_p = \mathcal{O}_{M,p}$. In fact, if $\mathfrak{F} \not\subset p\mathcal{O}_M$ then there is an element $\alpha \in \mathfrak{F}$ such that $\alpha \notin p\mathcal{O}_M$. Every element of $\mathcal{O}_{M,p}$ can be written as a unit of $\mathcal{O}_{M,p}$ times a power of p . Since $\alpha \notin p\mathcal{O}_M$ we have $\alpha \in \mathcal{O}_{M,p}^\times$, which implies $\alpha \mathcal{O}_{M,p} = \mathcal{O}_{M,p}$. Then, as $\alpha \in \mathfrak{F}$ it follows that

$$\mathcal{O}_{M,p} = \alpha \mathcal{O}_{M,p} \subset \mathcal{O}_p.$$

It is clear that $\mathcal{O}_p \subset \mathcal{O}_{M,p}$. Since $\mathfrak{F} \subset p\mathcal{O}_M$ for only finitely many primes p , the lemma follows. \square

Let F be a number field. A prime number p is called *non-decomposed* in F if there is only one place in F lying above p .

Lemma 1.7 *A number field F embeds into $M(\mathbb{Q})$ if and only if $[F : \mathbb{Q}] = 1, 2$ or 4 and p is non-decomposed in F for all $p \in S$.*

Proof: The statement about the degree of F is Proposition 1.1 (c). The case $F = \mathbb{Q}$ is trivial.

Let F be a quartic field and suppose that F embeds into $M(\mathbb{Q})$, then F is a strictly maximal subfield of $M(\mathbb{Q})$. We say that a subfield K of $M(\mathbb{Q})$ is a *splitting field* for $M(\mathbb{Q})$ (or that K *splits* $M(\mathbb{Q})$) if $M(\mathbb{Q}) \otimes K \cong \text{Mat}_4(K)$. Proposition 1.2(d) tells us that a quartic field embeds into $M(\mathbb{Q})$ if and only if it splits $M(\mathbb{Q})$.

For p a rational prime, the field \mathbb{Q}_p is an extension of \mathbb{Q} . Hence, by Proposition 1.1(c), the \mathbb{Q}_p -algebra $M(\mathbb{Q}_p)$ is central simple over \mathbb{Q}_p . Let $p \in S$. The Schur index, $\text{Ind } M(\mathbb{Q}_p)$, of $M(\mathbb{Q}_p)$ is, by [28], Corollary 17.10a(iii), equal to the order of $[M(\mathbb{Q}_p)]$ in the Brauer group of \mathbb{Q}_p , where the square brackets denote the Morita equivalence class. By choice of $M(\mathbb{Q})$ we have $\text{Ind } M(\mathbb{Q}_p) = 4$. Let \mathfrak{p}_i be the (finitely many) primes in F above p . Then Theorem 32.15 of [31] tells us that, since F splits $M(\mathbb{Q})$,

$$4 = \text{Ind } M(\mathbb{Q}_p) \mid [F_{\mathfrak{p}_i} : \mathbb{Q}_p]$$

for all i . Corollary 8.4 of Chapter II of [27] says that

$$[F : \mathbb{Q}] = \sum_i [F_{\mathfrak{p}_i} : \mathbb{Q}_p], \quad (2)$$

which implies that there is only one prime \mathfrak{p} in F above p and that $[F_{\mathfrak{p}} : \mathbb{Q}_p] = 4$.

Conversely, suppose that for each $p \in S$ there is only one prime \mathfrak{p} in F above p . From (2) we get that $[F_{\mathfrak{p}} : \mathbb{Q}_p] = 4$, so

$$\text{Ind } M(\mathbb{Q}_p) \mid [F_{\mathfrak{p}} : \mathbb{Q}_p]. \quad (3)$$

For $p \notin S$, by choice of $M(\mathbb{Q})$, the Schur index, $\text{ind } M(\mathbb{Q}_p)$, is equal to 1, so in this case (3) also holds for each \mathfrak{p} in F above p . Then, by [31], Theorem 32.15, the field F splits $M(\mathbb{Q})$. By Proposition 1.2(d) we then deduce that F embeds into $M(\mathbb{Q})$.

Now let F be a quadratic field and suppose that F embeds into $M(\mathbb{Q})$, then we consider F as a subfield of $M(\mathbb{Q})$. By Proposition 1.2(c), the subfield F of $M(\mathbb{Q})$ is not maximal so there exists a maximal subfield K of $M(\mathbb{Q})$ properly containing F , which by the same proposition is quartic. It was shown above that every prime in S is non-decomposed in K and hence also in F .

Suppose p is non-decomposed in F for all $p \in S$. We choose a quaternion algebra A over F by specifying that the local Brauer invariant at \mathfrak{p} be $\frac{1}{2}$ for all places \mathfrak{p} in F over some $p \in S$, and that the

local Brauer invariant be 0 at all other places of F . Proposition 1.2(c) tells us that there exists a subfield K of A containing F with $[K : F] = 2$. Then by the same argument as above, if \mathfrak{p} is a place of F over p for some $p \in S$, then \mathfrak{p} is non-decomposed in K . It follows that p is non-decomposed in K for all $p \in S$. It was shown above that the quartic extension K of \mathbb{Q} , and thus also the subfield F of K , embeds into $M(\mathbb{Q})$. The lemma is proven. \square

Let \mathbb{A}_{fin} denote the ring of finite adeles over \mathbb{Q} , ie.

$$\mathbb{A}_{\text{fin}} = \prod_p' \mathbb{Q}_p,$$

where p ranges over the rational primes and \prod_p' denotes the restricted product, that is, almost all components of a given element are integral. Let $\hat{\mathbb{Z}} = \prod_p \mathbb{Z}_p \subset \mathbb{A}_{\text{fin}}$. There is a natural embedding of \mathbb{Q} into \mathbb{A}_{fin} , which maps $q \in \mathbb{Q}$ to the adele every one of whose components is q . From this embedding we derive an embedding of $M(\mathbb{Q})$ in $M(\mathbb{A}_{\text{fin}})$ and an embedding of $\mathcal{G}(\mathbb{Q})$ in $\mathcal{G}(\mathbb{A}_{\text{fin}})$.

Lemma 1.8 $M(\mathbb{A}_{\text{fin}})^\times = M(\hat{\mathbb{Z}})^\times M(\mathbb{Q})^\times$.

Proof: We have the following commutative diagram with exact rows:

$$\begin{array}{ccccccc} 1 & \longrightarrow & \mathcal{G}(\mathbb{Q}) & \longrightarrow & M(\mathbb{Q})^\times & \xrightarrow{\det} & \mathbb{Q}^\times \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & \mathcal{G}(\mathbb{A}_{\text{fin}}) & \longrightarrow & M(\mathbb{A}_{\text{fin}})^\times & \xrightarrow{\det} & \mathbb{A}_{\text{fin}}^\times \longrightarrow 1 \\ & & \uparrow & & \uparrow & & \uparrow \\ 1 & \longrightarrow & \mathcal{G}(\hat{\mathbb{Z}}) & \longrightarrow & M(\hat{\mathbb{Z}})^\times & \xrightarrow{\det} & \hat{\mathbb{Z}}^\times \longrightarrow 1 \end{array}$$

where the vertical arrows denote the natural embeddings. The commutativity of the diagram and the exactness of the rows are clear, except that the surjectivity of the three determinant maps requires justification. The surjectivity of the map $\det : M(\mathbb{Q})^\times \rightarrow \mathbb{Q}^\times$ follows from [31], Theorem 33.15. For all primes p we have that $M(\mathbb{Q}_p)$ is a central simple \mathbb{Q}_p -algebra so it follows from [31], Theorem 33.4 that the map $\det : M(\mathbb{Q}_p)^\times \rightarrow \mathbb{Q}_p^\times$ is surjective. For $p \in S$, we have that $M(\mathbb{Q}_p)$ is a division \mathbb{Q}_p -algebra and so an element x of $M(\mathbb{Q}_p)$ is in $M(\mathbb{Z}_p)$ if and only if $\det x \in \mathbb{Z}_p$ ([31], Theorem 12.5). For $p \notin S$, we have that $M(\mathbb{Q}_p) \cong \text{Mat}_4(\mathbb{Q}_p)$ and

$$\det \begin{pmatrix} x & & & \\ & 1 & & \\ & & 1 & \\ & & & 1 \end{pmatrix} = x$$

for all $x \in \mathbb{Z}_p$. It follows that the map $\det : M(\hat{\mathbb{Z}})^\times \rightarrow \hat{\mathbb{Z}}^\times$ is surjective. From this we can then see that map $\det : M(\mathbb{A}_{\text{fin}})^\times \rightarrow \mathbb{A}_{\text{fin}}^\times$ is also surjective.

Let $v \in M(\mathbb{A}_{\text{fin}})^\times$ and let $w = \det v \in \mathbb{A}_{\text{fin}}^\times$. Since $\mathbb{A}_{\text{fin}}^\times = \hat{\mathbb{Z}}^\times \mathbb{Q}^\times$, there exist $r \in \hat{\mathbb{Z}}^\times$ and $q \in \mathbb{Q}^\times$ such that $w = rq$. By the surjectivity of \det , there exist $\bar{r} \in M(\hat{\mathbb{Z}})^\times$ and $\bar{q} \in M(\mathbb{Q})^\times$ such that $\det \bar{r} = r$ and $\det \bar{q} = q$. Let $\bar{v} = \bar{r}^{-1}v\bar{q}^{-1}$. Then $\det \bar{v} = 1$, so $\bar{v} \in \mathcal{G}(\mathbb{A}_{\text{fin}})$. By the Strong Approximation Theorem (see [25]), we have that $\mathcal{G}(\mathbb{Q})$ is dense in $\mathcal{G}(\mathbb{A}_{\text{fin}})$. Hence there exist $\hat{r} \in \mathcal{G}(\hat{\mathbb{Z}})$ and $\hat{q} \in \mathcal{G}(\mathbb{Q})$ such that $\bar{v} = \hat{r}\hat{q}$. Finally, we have

$$v = \bar{r}\bar{v}\bar{q} = \bar{r}(\hat{r}\hat{q})\bar{q} = (\bar{r}\hat{r})(\hat{q}\bar{q}),$$

where $\bar{r}\hat{r} \in M(\hat{\mathbb{Z}})^\times$ and $\hat{q}\bar{q} \in M(\mathbb{Q})^\times$. The lemma follows. \square

Lemma 1.9 Let F be a field that embeds into $M(\mathbb{Q})$. For each embedding $\sigma : F \rightarrow M(\mathbb{Q})$ the order $\mathcal{O}_\sigma = \sigma^{-1}(\sigma(F) \cap M(\mathbb{Z}))$ is maximal at all $p \in S$. Conversely, if \mathcal{O} is an order in the field F which is maximal at all $p \in S$, then there exists an embedding $\sigma : F \rightarrow M(\mathbb{Q})$ such that $\mathcal{O} = \mathcal{O}_\sigma$.

Let $\sigma : F \rightarrow M(\mathbb{Q})$ be an embedding of the field F into $M(\mathbb{Q})$. By Lemma 1.7 each prime p in the set S is non-split in F . Since for $p \in S$ there is only one place in F above p , we can note that the p -adic completion $F_p = F \otimes \mathbb{Q}_p$ is again a field (see [27], Chapter 1, Proposition 8.3). Firstly we need to show that for all $p \in S$, the completion $\mathcal{O}_{\sigma,p} = \mathcal{O}_\sigma \otimes \mathbb{Z}_p$ is the maximal order in F_p . By Proposition 1.3(c),

$M(\mathbb{Z}_p)$ is the maximal \mathbb{Z}_p -order in $M(\mathbb{Q}_p)$. Since $M(\mathbb{Q}_p)$ is a division algebra, $M(\mathbb{Z}_p)$ coincides with the integral closure of \mathbb{Z}_p in $M(\mathbb{Q}_p)$, by Proposition 1.3(d). We can extend σ to an embedding of F_p in $M(\mathbb{Q}_p)$ and then $\mathcal{O}_{\sigma,p} = \sigma^{-1}(\sigma(F_p) \cap M(\mathbb{Z}_p))$ is the integral closure of \mathbb{Z}_p in F_p , which is the maximal order of F_p .

For the converse, let \mathcal{O} be an order of F such that the completion \mathcal{O}_p is maximal for each $p \in S$. Via σ we consider F to be a subfield of $M(\mathbb{Q})$. For any $u \in M(\mathbb{Q})^\times$ let $\mathcal{O}_u = F \cap u^{-1}M(\mathbb{Z})u$. Let ${}^u\sigma = u\sigma u^{-1}$, that is: ${}^u\sigma(x) = u\sigma(x)u^{-1}$ for all $x \in F$. We will show that there is a $u \in M(\mathbb{Q})^\times$ such that $\mathcal{O} = \mathcal{O}_u$. The embedding ${}^u\sigma$ is then the one required by the lemma.

Let $\mathcal{O}_1 = F \cap M(\mathbb{Z})$. Since \mathcal{O} and \mathcal{O}_1 are orders, by Lemma 1.6 they are both maximal at all but finitely many places. Let T be the set of primes p such that either \mathcal{O} or \mathcal{O}_1 is not maximal at p . Then T is finite and $T \cap S = \emptyset$. Furthermore, if T_F denotes the set of places of F lying over T , we have that for any place \mathfrak{p} of F with $\mathfrak{p} \notin T_F$ the completions $\mathcal{O}_{\mathfrak{p}}$ and $\mathcal{O}_{1,\mathfrak{p}}$ are maximal in $F_{\mathfrak{p}}$ and thus equal, by uniqueness of maximal orders. Hence, for $p \notin T$ we have

$$\mathcal{O}_p = F_p \cap M(\mathbb{Z}_p).$$

Let $p \in T$, then $p \notin S$ so $M(\mathbb{Q}_p) \cong \text{Mat}_4(\mathbb{Q}_p)$. Considering F_p as a \mathbb{Q}_p -vector space we see that we can embed F_p into $\text{Lin}_{\mathbb{Q}_p}(F_p, F_p)$ by sending an element $x \in F_p$ to the linear map $a \mapsto ax$. We choose a \mathbb{Z}_p -basis of \mathcal{O}_p , which is then also a \mathbb{Q}_p -basis of F_p . This gives us an isomorphism

$$\text{Lin}_{\mathbb{Q}_p}(F_p, F_p) \cong \text{Mat}_4(\mathbb{Q}_p) \cong M(\mathbb{Q}_p).$$

This isomorphism and the above embedding $F_p \hookrightarrow \text{Lin}_{\mathbb{Q}_p}(F_p, F_p)$ then give us an embedding $\sigma_p : F_p \hookrightarrow M(\mathbb{Q}_p)$ such that $\mathcal{O}_p = \sigma_p^{-1}(\sigma_p(F_p) \cap M(\mathbb{Z}_p))$. The map σ_p is a \mathbb{Q}_p -isomorphism of F_p (considered as a subfield of $M(\mathbb{Q}_p)$ via a suitable extension of σ) onto its image in $M(\mathbb{Q}_p)$, so by the Skolem-Noether Theorem (Proposition 1.3(a)), there exists $u_p \in M(\mathbb{Q}_p)^\times$ such that $u_p x u_p^{-1} = \sigma_p(x)$ for all $x \in F_p$. Hence

$$\mathcal{O}_p = F_p \cap u_p^{-1}M(\mathbb{Z}_p)u_p.$$

For $p \notin T$ set $u_p = 1$ and let $\tilde{u} = (u_p) \in \mathbb{A}_{\text{fin}}$. By Lemma 1.8

$$M(\mathbb{A}_{\text{fin}})^\times = M(\hat{\mathbb{Z}})^\times M(\mathbb{Q})^\times$$

so there exists an element $u \in M(\mathbb{Q})^\times$ such that for all primes p we have $u^{-1}M(\mathbb{Z}_p)u = u_p^{-1}M(\mathbb{Z}_p)u_p$. This implies that

$$\mathcal{O}_p = F_p \cap u^{-1}M(\mathbb{Z}_p)u \tag{4}$$

for all primes p and we deduce that $\mathcal{O} = F \cap u^{-1}M(\mathbb{Z})u = \mathcal{O}_u$. This completes the proof of the lemma. \square

1.5 Counting order embeddings

Let F/\mathbb{Q} be an algebraic number field and let \mathcal{O} be an order in F . Let $I(\mathcal{O})$ be the set of all finitely generated \mathcal{O} -submodules of F . According to the Jordan-Zassenhaus Theorem ([31], Theorem 26.4), the set $[I(\mathcal{O})]$ of isomorphism classes of elements of $I(\mathcal{O})$ is finite. Let $h(\mathcal{O})$ be the cardinality of the set $[I(\mathcal{O})]$, called the *class number* of \mathcal{O} .

Let I be a non-trivial, finitely generated \mathcal{O} -submodule of F . Then, by [31], Theorem 10.6, I is isomorphic as an \mathcal{O} -module to an ideal of \mathcal{O} so also has the property that $I \otimes \mathbb{Q} = F$. If J is another finitely generated \mathcal{O} -submodule of F , such that $J \cong I$, then the isomorphism extends to an automorphism of F considered as a module over itself, and hence $J = Ix$ for some $x \in F^\times$. So $h(\mathcal{O}) = \text{card}([I(\mathcal{O})]) = |I(\mathcal{O})/F^\times|$.

For a prime $p \in \mathbb{Z}$ let $F_p = F \otimes \mathbb{Q}_p$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the prime ideals of F above p . By [27], Chapter 1, Proposition 8.3 there exists a canonical \mathbb{Q}_p -algebra isomorphism defined by:

$$\begin{aligned} F_p = F \otimes \mathbb{Q}_p &\cong \prod_{i=1}^n F_{\mathfrak{p}_i} \\ \alpha \otimes x &\mapsto (\tau_i(\alpha).x)_{i=1}^n, \end{aligned} \tag{5}$$

where $F_{\mathfrak{p}_i}$ denotes the completion of F with respect to the \mathfrak{p}_i -adic absolute value and τ_i the embedding of F into $F_{\mathfrak{p}_i}$. If \mathcal{O} is an order in F and $p \in \mathbb{Z}$ a prime then let $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$.

Recall that S is a finite, non-empty set of prime numbers with an even number of elements. Let $C(S)$ be the set of all totally complex quartic fields F such that all primes p in S are non-decomposed in F . Note in particular that by the isomorphism (5) this means that for each field F in $C(S)$ and for each $p \in S$ we have that $F_p = F \otimes \mathbb{Q}_p$ is once again a field, namely the completion of F at the unique place of F above p . For $F \in C(S)$ let $O_F(S)$ be the set of isomorphism classes of orders \mathcal{O} in F which are maximal at all $p \in S$, ie. are such that the completion $\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p$ is the maximal order of the field F_p for all $p \in S$. Let $O(S)$ be the union of all $O_F(S)$, where F ranges over $C(S)$.

Let $F \in C(S)$ and $\mathcal{O} \in O_F(S)$, then, by Lemma 1.7, F embeds into $M(\mathbb{Q})$. By Lemma 1.5, the group $M(\mathbb{Z})^\times$ of units in $M(\mathbb{Z})$ contains Γ as a subgroup. By Lemma 1.9 we know that there is an embedding σ of F into $M(\mathbb{Q})$ such that $\mathcal{O} = \mathcal{O}_\sigma = \sigma^{-1}(\sigma(F) \cap M(\mathbb{Z}))$. Let $u \in M(\mathbb{Z})^\times$ and, as above, let ${}^u\sigma = u\sigma u^{-1}$ for embeddings $\sigma : F \rightarrow M(\mathbb{Q})$. Then $\mathcal{O}_{u\sigma} = \mathcal{O}_\sigma$, so the group $M(\mathbb{Z})^\times$ acts on the set $\Sigma(\mathcal{O})$ of all embeddings σ with $\mathcal{O}_\sigma = \mathcal{O}$. This $M(\mathbb{Z})^\times$ action also restricts to an action of Γ on $\Sigma(\mathcal{O})$.

We define

$$\lambda_S(\mathcal{O}) = \lambda_S(F) = \prod_{p \in S} f_p(F),$$

where $f_p(F)$ is the inertia degree of p in F . Our aim is to prove the following proposition.

Proposition 1.10 *The quotient $M(\mathbb{Z})^\times \backslash \Sigma(\mathcal{O})$ is finite and has cardinality $h(\mathcal{O})\lambda_S(\mathcal{O})$.*

We prepare for the proof of the proposition with the following discussion and then prove some lemmas, from which the proposition will follow.

Fix an embedding $\sigma : F \hookrightarrow M(\mathbb{Q})$ with $\mathcal{O} = \mathcal{O}_\sigma$ and consider F as a subfield of $M(\mathbb{Q})$ such that $\mathcal{O} = F \cap M(\mathbb{Z})$. For $u \in M(\mathbb{Q})^\times$ let $\mathcal{O}_u = F \cap u^{-1}M(\mathbb{Z})u$. Let U be the set of all $u \in M(\mathbb{Q})^\times$ such that $\mathcal{O} = F \cap M(\mathbb{Z}) = F \cap u^{-1}M(\mathbb{Z})u = \mathcal{O}_u$. Let $a \in F^\times$, then

$$F \cap a^{-1}u^{-1}M(\mathbb{Z})ua = a^{-1}(F \cap u^{-1}M(\mathbb{Z})u)a = F \cap u^{-1}M(\mathbb{Z})u,$$

so F^\times acts on U by multiplication from the right. Let $v \in M(\mathbb{Z})^\times$, then

$$F \cap u^{-1}v^{-1}M(\mathbb{Z})vu = F \cap u^{-1}M(\mathbb{Z})u,$$

so $M(\mathbb{Z})^\times$ acts on U by multiplication from the left. Let $\tau \in \Sigma(\mathcal{O})$, so that $\mathcal{O}_\tau = \mathcal{O}$. Then by the Skolem-Noether Theorem (Proposition 1.3(a)) there exists $u \in M(\mathbb{Q})$ such that $\tau = {}^u\sigma = u\sigma u^{-1}$, ie. $\tau(F) = uFu^{-1}$. Then

$$\begin{aligned} \mathcal{O}_u = F \cap u^{-1}M(\mathbb{Z})u &= u^{-1}(uFu^{-1} \cap M(\mathbb{Z}))u \\ &= u^{-1}(\tau(F) \cap M(\mathbb{Z}))u \\ &= \mathcal{O}_\tau = \mathcal{O}. \end{aligned}$$

Conversely, it is clear that for all $u \in U$ we have ${}^u\sigma \in \Sigma(\mathcal{O})$, and that ${}^u\sigma = {}^v\sigma$ if and only if $u = vx$ for some $x \in F^\times$. Hence

$$|M(\mathbb{Z})^\times \backslash U/F^\times| = |M(\mathbb{Z})^\times \backslash \Sigma(\mathcal{O})|,$$

and the proposition will be proved if we can show that the left hand side equals $h(\mathcal{O})\lambda_S(\mathcal{O})$.

For $u \in U$ let

$$I_u = F \cap M(\mathbb{Z})u.$$

Then I_u is a finitely generated \mathcal{O} -module in F . We shall prove that the map

$$\begin{aligned} \Psi : M(\mathbb{Z})^\times \backslash U/F^\times &\rightarrow I(\mathcal{O})/F^\times \\ u &\mapsto I_u, \end{aligned}$$

is surjective and $\lambda_S(\mathcal{O})$ to one. This will be done in the following lemmas through localisation and strong approximation.

Let $p \in \mathbb{Z}$ be a prime and let $I(\mathcal{O}_p)$ be the set of all finitely generated \mathcal{O}_p -submodules of F_p and $[I(\mathcal{O}_p)]$ the set of isomorphism classes. Let I_p be a non-trivial, finitely generated \mathcal{O}_p -submodule of F_p . Then, by [31], Theorem 10.6, the submodule I_p is isomorphic as an \mathcal{O}_p -module to an ideal of \mathcal{O}_p so also has the property that $I_p \otimes \mathbb{Q}_p = F_p$. If J_p is another finitely generated \mathcal{O}_p -submodule of F_p , such that $J_p \cong I_p$, then the isomorphism extends to an automorphism of F_p considered as a module over itself, and hence $J_p = I_p x$ for some $x \in F_p^\times$. So $\text{card}([I(\mathcal{O}_p)]) = |I(\mathcal{O}_p)/F_p^\times|$.

For a prime p and $u_p \in M(\mathbb{Q}_p)^\times$ let $\mathcal{O}_{p,u_p} = F_p \cap u_p^{-1}M(\mathbb{Z}_p)u_p$ and recall that $\mathcal{O}_p = F_p \cap M(\mathbb{Z}_p)$. Let U_p be the set of all $u_p \in M(\mathbb{Q}_p)^\times$ such that $\mathcal{O}_{p,u_p} = \mathcal{O}_p$.

As in the global case above, F_p^\times acts on U_p from the right and $M(\mathbb{Z}_p)^\times$ acts on U_p from the left. For $u_p \in U_p$ let

$$I_{u_p} = F_p \cap M(\mathbb{Z}_p)u_p.$$

Then I_{u_p} is a finitely generated \mathcal{O}_p -module in F_p .

Lemma 1.11 *Let p be a prime. Then $|I(\mathcal{O}_p)/F_p^\times| = 1$.*

Proof: Suppose $p \in S$. Then p is non-decomposed in F so there exists a unique prime ideal \mathfrak{p} of F above p , so by the isomorphism (5) we can see that $F_p \cong F_{\mathfrak{p}}$ and hence F_p is itself a field. By [27], Chapter II, Proposition 3.9, every ideal of \mathcal{O}_p is principal and hence all non-zero ideals of \mathcal{O}_p are isomorphic. The claim holds for $p \in S$.

Suppose $p \notin S$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the prime ideals of F over p . Under the isomorphism (5) an ideal in \mathcal{O}_p gives ideals in $\mathcal{O}_{\mathfrak{p}_1}, \dots, \mathcal{O}_{\mathfrak{p}_n}$, where $\mathcal{O}_{\mathfrak{p}_1}$ denotes the ring of integers in the field $F_{\mathfrak{p}_1}$. As we saw above, these ideals are each unique up to isomorphism and hence the original ideal in \mathcal{O}_p is also unique up to isomorphism and the claim holds for $p \notin S$. \square

We now prove the surjectivity of Ψ .

Lemma 1.12 *The map Ψ is surjective.*

Proof: Let $I \subset \mathcal{O}$ be an ideal and for a prime p let $I_p = I \otimes \mathbb{Z}_p$. By Lemma 1.11, for all primes p the \mathcal{O}_p -module $F_p \cap M(\mathbb{Z}_p)$ is isomorphic to I_p , so there exists $u_p \in F_p^\times$ such that $F_p \cap M(\mathbb{Z}_p)u_p = I_p$. We have further that $F_p \cap u_p^{-1}M(\mathbb{Z}_p)u_p = u_p^{-1}(F_p \cap M(\mathbb{Z}_p)u_p) = F_p \cap M(\mathbb{Z}_p)$.

Let $\tilde{u} = (u_p) \in \mathbb{A}_{\text{fin}}^\times$. By Lemma 1.8 there exist $\tilde{z} \in M(\hat{\mathbb{Z}})^\times$ and $u \in M(\mathbb{Q})^\times$ such that $\tilde{u} = \tilde{z}u$. Then for all primes p we have that $F_p \cap u^{-1}M(\mathbb{Z}_p)u = F_p \cap M(\mathbb{Z}_p)$ and $F_p \cap M(\mathbb{Z}_p)u = I_p$. We deduce from this that $F \cap u^{-1}M(\mathbb{Z})u = F \cap M(\mathbb{Z})$ and $F \cap M(\mathbb{Z})u = I$. This is what was required to complete the proof of the lemma. \square

In the following series of lemmas we prove that Ψ is $\lambda_S(\mathcal{O})$ to one.

Lemma 1.13 *Let K be a non-archimedean local field and \mathcal{O}_K its ring of integers. For $n \in \mathbb{N}$ let $\Delta_n \subset \text{Mat}_n(K)$ be the subspace of diagonal matrices and suppose that $u \in \text{GL}_n(K)$ is such that*

$$\Delta_n \cap \text{Mat}_n(\mathcal{O}_K) \subset \Delta_n \cap u^{-1}\text{Mat}_n(\mathcal{O}_K)u.$$

Then there exist $z \in \text{Mat}_n(\mathcal{O}_K)^\times$ and $x \in \Delta_n^\times$ such that $zu = x$.

If we suppose further that

$$\Delta_n \cap \text{Mat}_n(\mathcal{O}_K) = \Delta_n \cap \text{Mat}_n(\mathcal{O}_K)u$$

then we have $x \in (\Delta_n \cap \text{Mat}_n(\mathcal{O}_K))^\times$.

Proof: The first claim of the lemma will be proved by induction on n . For $n = 1$ we take $z = 1$ and $x = u$ and the claim holds. Assume now that the claim holds for some $n - 1 \in \mathbb{N}$. For any ring R let $\text{Upp}_n(R)$ denote the subalgebra of upper triangular matrices in $\text{Mat}_n(R)$. We can choose an element $y \in \text{Mat}_n(\mathcal{O}_K)^\times$ such that $u' = yu \in \text{Upp}_n(K)$ is upper triangular. Then u' has the form

$$u' = \begin{pmatrix} a & b \\ & c \end{pmatrix},$$

where $a \in K$, $b \in \text{Mat}_{1 \times (n-1)}(K)$ and $c \in \text{Upp}_{n-1}(K)$. Then

$$(u')^{-1} = \begin{pmatrix} a^{-1} & -a^{-1}bc^{-1} \\ & c^{-1} \end{pmatrix}.$$

Since u satisfies $\Delta_n \cap \text{Mat}_n(\mathcal{O}_K) \subset \Delta_n \cap u^{-1}\text{Mat}_n(\mathcal{O}_K)u$, it follows that u' satisfies $\Delta_n \cap \text{Upp}_n(\mathcal{O}_K) \subset \Delta_n \cap (u')^{-1}\text{Upp}_n(\mathcal{O}_K)u'$. It follows that there exist $\alpha \in \mathcal{O}_K$, $\beta \in \text{Mat}_{1 \times (n-1)}(\mathcal{O}_K)$ and $\gamma \in \text{Upp}_{n-1}(\mathcal{O}_K)$ such that

$$\begin{pmatrix} \alpha & a^{-1}(\alpha b + \beta c - bc^{-1}\gamma c) \\ & c^{-1}\gamma c \end{pmatrix} = (u')^{-1} \begin{pmatrix} \alpha & \beta \\ & \gamma \end{pmatrix} u' = \begin{pmatrix} 1 & \\ & 0 \end{pmatrix},$$

where the matrix on the right is the n by n matrix with a one in the top left corner and all other entries zero. It then follows that $\alpha = 1$, $c^{-1}\gamma c = 0$ and $b = -\beta c$. Let

$$w = \begin{pmatrix} 1 & \beta \\ & I_{n-1} \end{pmatrix} \in \text{Mat}_n(\mathcal{O}_K)^\times.$$

Then

$$wu' = \begin{pmatrix} 1 & \beta \\ & I_{n-1} \end{pmatrix} \begin{pmatrix} a & -\beta c \\ & c \end{pmatrix} = \begin{pmatrix} a & \\ & c \end{pmatrix}.$$

so we have that

$$wyu = \begin{pmatrix} a & \\ & c \end{pmatrix}.$$

It is then clear that c satisfies

$$\Delta_{n-1} \cap \text{Mat}_{n-1}(\mathcal{O}_K) \subset \Delta_{n-1} \cap c^{-1}\text{Mat}_{n-1}(\mathcal{O}_K)c$$

so by the inductive hypothesis there exist $z' \in \text{Mat}_{n-1}(\mathcal{O}_K)^\times$ and $x' \in \Delta_{n-1}^\times$ such that $z'c = x'$. Setting

$$z = \begin{pmatrix} 1 & \\ & z' \end{pmatrix} wy \in \text{Mat}_n(\mathcal{O}_K)^\times \quad \text{and} \quad x = \begin{pmatrix} a & \\ & x' \end{pmatrix} \in \Delta_n^\times$$

we get that $zu = x$ and the proof of the first claim is complete.

If we also assume that u satisfies

$$\Delta_n \cap \text{Mat}_n(\mathcal{O}_K) = \Delta_n \cap \text{Mat}_n(\mathcal{O}_K)u$$

then since $z \in \text{Mat}_n(\mathcal{O}_K)^\times$ and $zu = x \in \Delta_n^\times$ it follows that

$$\Delta_n \cap \text{Mat}_n(\mathcal{O}_K) = \Delta_n \cap \text{Mat}_n(\mathcal{O}_K)zu = (\Delta_n \cap \text{Mat}_n(\mathcal{O}_K))x.$$

This can be the case only if $x \in (\Delta_n \cap \text{Mat}_n(\mathcal{O}_K))^\times$ so the lemma is proved. \square

Lemma 1.14 *For $p \notin S$ we have $|M(\mathbb{Z}_p)^\times \backslash U_p / F_p^\times| = 1$.*

Proof: Let $p \notin S$ and let $u_p \in U_p$ so that

$$F_p \cap M(\mathbb{Z}_p) = F_p \cap u_p^{-1}M(\mathbb{Z}_p)u_p. \quad (6)$$

By Lemma 1.11, there exists $\lambda_p \in F_p^\times$ such that $F_p \cap M(\mathbb{Z}_p) = F_p \cap M(\mathbb{Z}_p)u_p\lambda_p$. Replacing u_p with $u_p\lambda_p$ we may assume that u_p satisfies

$$F_p \cap M(\mathbb{Z}_p) = F_p \cap M(\mathbb{Z}_p)u_p. \quad (7)$$

We shall show that there exist $z_p \in M(\mathbb{Z}_p)^\times$ and $x_p \in F_p^\times$ such that $z_p u_p x_p$ is the identity element in $M(\mathbb{Q}_p)$.

Let ε be an integral element of F generating F over \mathbb{Q} , and let L be an extension of \mathbb{Q} containing all the zeros of the minimal polynomial of ε . Let $L_p = L \otimes \mathbb{Q}_p$, note that neither this nor F_p are necessarily fields, rather a finite direct product of fields. The embedding $F \hookrightarrow M(\mathbb{Q})$ gives us an embedding $F_p \hookrightarrow M(\mathbb{Q}_p)$. Since $p \notin S$ we have $M(\mathbb{Q}_p) \cong \text{Mat}_4(\mathbb{Q}_p)$ so we get an embedding

$$F_p \otimes L \hookrightarrow M(\mathbb{Q}_p) \otimes L \cong \text{Mat}_4(L_p).$$

Let \mathcal{O}_L be the ring of integers in L and let $\mathcal{O}_{L_p} = \mathcal{O}_L \otimes \mathbb{Z}_p$. Let Δ denote the subspace of diagonal matrices in $\text{Mat}_4(L_p)$. It follows from our choice of L that ε is diagonalisable in $M(L_p)$ by an element $A \in M(\mathcal{O}_{L_p})^\times$. Since $F_p = \mathbb{Q}_p(\varepsilon)$, the whole of $F_p \otimes L$ is simultaneously diagonalisable in $M(L_p)$, that is, we have that $A^{-1}(F_p \otimes L)A$ is a subspace of Δ , and by dimensional considerations we must have that $A^{-1}(F_p \otimes L)A = \Delta$. Then, tensoring (6) and (7) with \mathcal{O}_L and conjugating by A we get

$$\Delta \cap M(\mathcal{O}_{L_p}) = \Delta \cap \bar{u}_p^{-1}M(\mathcal{O}_{L_p})\bar{u}_p \quad (8)$$

and

$$\Delta \cap M(\mathcal{O}_{L_p}) = \Delta \cap M(\mathcal{O}_{L_p})\bar{u}_p, \quad (9)$$

where $\bar{u}_p = u_p A$.

We are currently working in the matrix algebra $M(L_p) \cong \text{Mat}_4(L_p)$. Let $\mathfrak{p}_1, \dots, \mathfrak{p}_n$ be the prime ideals of L above p . By virtue of the isomorphism (5) we can consider separately each \mathfrak{p}_i -adic component of the entries of the matrices. It then follows from Lemma 1.13 and equations (8) and (9) that there exist $\bar{z} \in M(\mathcal{O}_{L_p})^\times$ and $\bar{x} \in (\Delta \cap M(\mathcal{O}_{L_p}))^\times$ such that $\bar{z}\bar{u}_p = \bar{x}$. Setting $z = A\bar{z} \in M(\mathcal{O}_{L_p})^\times$ and $x = A\bar{x}A^{-1} \in ((F_p \otimes L) \cap M(\mathcal{O}_{L_p}))^\times$ we get that $zu_p = x$.

Consider now the trace map $\text{tr}_{L/\mathbb{Q}}$ of the field extension L/\mathbb{Q} . The image of \mathcal{O}_L under this map is an ideal in \mathbb{Z} . Let $\nu \in \mathbb{Z}$ be the greatest such that $\text{tr}_{L/\mathbb{Q}}(\mathcal{O}_L) \subset p^\nu \mathbb{Z}$. We define a linear map

$$\begin{aligned} T : M(L_p) = M(\mathbb{Q}_p) \otimes L &\rightarrow M(\mathbb{Q}_p) \otimes \mathbb{Q} \cong M(\mathbb{Q}_p) \\ x \otimes y &\mapsto x \otimes p^{-\nu}(\text{tr}_{L/\mathbb{Q}} y). \end{aligned}$$

Note that $T(M(\mathcal{O}_{L_p})) = T(M(\mathbb{Z}_p) \otimes \mathcal{O}_L) \subset M(\mathbb{Z}_p) \otimes \mathbb{Z} \cong M(\mathbb{Z}_p)$.

We denote by \mathcal{O}_{L_1} the ring of integers of the field $L_{\mathfrak{p}_1}$. Let $\xi \in (F \otimes L_{\mathfrak{p}_1}) \cap M(\mathcal{O}_{L_1})$ and let x_1 and z_1 be the \mathfrak{p}_1 components of x and z . Then $z_1 u_p = x_1$. Now set $\alpha = x_1^{-1} \xi \in (F \otimes L_{\mathfrak{p}_1}) \cap M(\mathcal{O}_{L_1})$. From (6) we deduce that

$$(F \otimes L_{\mathfrak{p}_1}) \cap M(\mathcal{O}_{L_1}) = (F \otimes L_{\mathfrak{p}_1}) \cap u_p^{-1} M(\mathcal{O}_{L_1}) u_p$$

so there exists $\beta \in M(\mathcal{O}_{L_1})$ such that $\alpha = u_p^{-1} \beta u_p$, or equivalently $u_p \alpha = \beta u_p$. Setting $\zeta = z_1 \beta \in M(\mathcal{O}_{L_1})$, we then get

$$\zeta u_p = z_1 \beta u_p = z_1 u_p \alpha = x_1 \alpha = \xi.$$

Hence we can see that $\xi u_p^{-1} \in M(\mathcal{O}_{L_1})$.

We now consider the linear map defined by

$$\begin{aligned} T' : M(\mathbb{Q}) \otimes L_{\mathfrak{p}_1} &\rightarrow M(\mathbb{Q}) \otimes \mathbb{Q}_p = M(\mathbb{Q}_p) \\ x \otimes y &\mapsto x \otimes p^{-\nu}(\text{tr}_{L_{\mathfrak{p}_1}/\mathbb{Q}_p} y), \end{aligned}$$

where $\text{tr}_{L_{\mathfrak{p}_1}/\mathbb{Q}_p}$ is the trace map of the field extension $L_{\mathfrak{p}_1}/\mathbb{Q}_p$. We note that T' maps $(F \otimes L_{\mathfrak{p}_1}) \cap M(\mathcal{O}_{L_p})$ to $F_p \cap M(\mathbb{Z}_p)$. The map T' induces a linear map

$$T'' : \frac{M(\mathcal{O}_{L_1})}{\mathfrak{p}_1 M(\mathcal{O}_{L_1})} \rightarrow \frac{M(\mathbb{Z}_p)}{pM(\mathbb{Z}_p)}.$$

Note that $M(\mathcal{O}_{L_1})/\mathfrak{p}_1 M(\mathcal{O}_{L_1})$ is a vector space over the field $\mathcal{O}_{L_1}/\mathfrak{p}_1 \mathcal{O}_{L_1}$ and $M(\mathbb{Z}_p)/pM(\mathbb{Z}_p)$ is a vector space over the field $\mathbb{Z}_p/p\mathbb{Z}_p \cong \mathbb{F}_p$. By the choice of the integer ν we can see that the map T'' is not the zero map, that is, its kernel is a proper subspace of $M(\mathcal{O}_{L_1})/\mathfrak{p}_1 M(\mathcal{O}_{L_1})$. An element of $M(\mathcal{O}_{L_1})/\mathfrak{p}_1 M(\mathcal{O}_{L_1})$ not in the kernel of T'' corresponds to an element of $M(\mathcal{O}_{L_1})$ whose image under T' is in $M(\mathbb{Z}_p)^\times$. We choose an element $\xi \in (F \otimes L_{\mathfrak{p}_1}) \cap M(\mathcal{O}_{L_1})$ such that $T'(\xi) \in (F_p \cap M(\mathbb{Z}_p))^\times$ and $T'(\xi u_p^{-1}) \in M(\mathbb{Z}_p)^\times$.

We shall write ξ also for the element of $(F_p \otimes L) \cap M(\mathcal{O}_{L_p})$ with \mathfrak{p}_1 component equal to ξ and all other components zero. Similarly we denote by ζ the element of $M(\mathcal{O}_{L_p})$ with \mathfrak{p}_1 component equal to ξu_p^{-1} and all other components zero. Then $\zeta u_p = \xi$. From the definitions of the maps T and T' and the isomorphism (5) it follows that $T(\xi) = T'(\xi') \in (F_p \cap M(\mathbb{Z}_p))^\times$ and $T(\zeta) = T'(\zeta) \in M(\mathbb{Z}_p)^\times$.

Now set $x_p = T(\xi) \in (F_p \cap M(\mathbb{Z}_p))^\times$ and $z_p = T(\zeta) \in M(\mathbb{Z}_p)^\times$. We then have that $z_p u_p = x_p$ and the lemma is proved. \square

Lemma 1.15 *For $p \in S$ we have $|M(\mathbb{Z}_p)^\times \setminus U_p/F_p^\times| = f_p(F)$.*

Proof: Let $p \in S$. We then have that $M(\mathbb{Q}_p)$ is a division algebra so in particular $M(\mathbb{Q}_p)^\times = M(\mathbb{Q}_p) \setminus \{0\}$. Further, since \mathbb{Q}_p is a local field, $M(\mathbb{Z}_p)$ is the unique maximal order of $M(\mathbb{Q}_p)$ (cf. Proposition 1.3(d)) and hence $u_p^{-1} M(\mathbb{Z}_p) u_p = M(\mathbb{Z}_p)$ for all $u_p \in M(\mathbb{Q}_p)^\times$. Thus the claim is equivalent to

$$|M(\mathbb{Z}_p)^\times \setminus M(\mathbb{Q}_p)^\times / F_p^\times| = f_p(F).$$

Let v_M be the p -adic valuation on $M(\mathbb{Q}_p)$ and let

$$e_M = e(M(\mathbb{Q}_p)/\mathbb{Q}_p) = |v_M(M(\mathbb{Q}_p)^\times)/v_M(\mathbb{Q}_p^\times)|$$

be the ramification index of \mathbb{Q}_p in $M(\mathbb{Q}_p)$. The valuation v_M is a surjective group homomorphism of $M(\mathbb{Q}_p)^\times$ onto \mathbb{Z} with kernel $M(\mathbb{Z}_p)^\times$. It follows that

$$e_M = |M(\mathbb{Z}_p)^\times \setminus M(\mathbb{Q}_p)^\times / \mathbb{Q}_p^\times|.$$

By Proposition 17.7 of [28] we have

$$|M(\mathbb{Z}_p)^\times \backslash M(\mathbb{Q}_p)^\times / \mathbb{Q}_p^\times| = e_M = \deg M(\mathbb{Q}_p) = 4.$$

Let $e_p(F)$ be the ramification index of p in F . Then by [27], Chapter I, Proposition 8.2, and since p does not split in F , we have

$$e_p(F)f_p(F) = [F : \mathbb{Q}] = 4. \quad (10)$$

Let \mathcal{O} be the valuation ring of F_p and let $\Pi = \pi\mathcal{O}$ be the unique maximal ideal of \mathcal{O} , where $\pi \in \mathcal{O}$ is a generator of the principal ideal Π . Let $\mathfrak{p} = p\mathbb{Z}_p$ be the unique maximal ideal of \mathbb{Z}_p . Then $\mathfrak{p} = \Pi \cap \mathbb{Z}_p$ and $p = \pi^{e_p(F)}$. Thus $v_M(\pi) = v_M(p)/e_p(F)$, which implies that

$$|M(\mathbb{Z}_p)^\times \backslash M(\mathbb{Q}_p)^\times / F_p^\times| = \frac{|M(\mathbb{Z}_p)^\times \backslash M(\mathbb{Q}_p)^\times / \mathbb{Q}_p^\times|}{e_p(F)} = \frac{4}{e_p(F)},$$

and hence from (10) we get

$$|M(\mathbb{Z}_p)^\times \backslash M(\mathbb{Q}_p)^\times / F_p^\times| = f_p(F),$$

as required. \square

Lemma 1.16 Ψ is $\lambda_S(\mathcal{O})$ to one.

Proof: Recall that $\mathcal{O} \in O_F(S)$ for some $F \in C(S)$. Let $\hat{F} = \prod'_p F_p$ be the restricted product over all primes p , that is, all but finitely many components are integral, and let \hat{U} be the set of all $\tilde{u} = (u_p) \in M(\mathbb{A}_{\text{fin}})^\times$ such that $\mathcal{O}_p = F_p \cap u_p^{-1}M(\mathbb{Z}_p)u_p = \mathcal{O}_{p,u_p}$ for all p .

For $I \in I(\mathcal{O})$ let $U_I = \Psi^{-1}(IF^\times)$. Let $u \in U_I$ for some $I \in I(\mathcal{O})$. We denote by \hat{u} the element of $M(\mathbb{A}_{\text{fin}})$ each of whose components is u . Setting $u_p = u$ for all primes p , we see that for all p

$$\mathcal{O}_p = \mathcal{O} \otimes \mathbb{Z}_p = \mathcal{O}_u \otimes \mathbb{Z}_p = \mathcal{O}_{p,u_p}$$

so $\hat{u} \in \hat{U}$.

For each $I \in I(\mathcal{O})$ we define the map

$$\Phi_I : M(\mathbb{Z})^\times \backslash U_I / F^\times \rightarrow M(\hat{\mathbb{Z}})^\times \backslash \hat{U} / \hat{F}^\times$$

by setting $\Phi_I(M(\mathbb{Z})^\times u F^\times) = M(\hat{\mathbb{Z}})^\times \hat{u} \hat{F}^\times$. We shall show that Φ_I is a bijection. Since from Lemmas 1.14 and 1.15 we know that $|M(\hat{\mathbb{Z}})^\times \backslash \hat{U} / \hat{F}^\times| = \lambda_S(\mathcal{O})$, the lemma will then follow.

First we show surjectivity. Let $\tilde{u} = (u_p) \in \hat{U}$, so that $\mathcal{O}_{p,u_p} = \mathcal{O}_p$ for all primes p . For all primes p , by Lemma 1.11 we have $I \otimes \mathbb{Q}_p \cong F_p \cap M(\mathbb{Z}_p)u_p$ so there exists $x_p \in F_p^\times$ such that $I \otimes \mathbb{Q}_p = F_p \cap M(\mathbb{Z}_p)u_p x_p$. We replace u_p with $u_p x_p$. By Lemma 1.8 there exist $\tilde{z} = (z_p) \in M(\hat{\mathbb{Z}})^\times$ and $u \in M(\mathbb{Q})^\times$ such that $\tilde{u} = \tilde{z}\hat{u}$. It follows that $\mathcal{O}_{p,u} = \mathcal{O}_p$ for all primes p and hence we get that $\mathcal{O}_u = \mathcal{O}$, so that $u \in U$. Furthermore, since

$$I \otimes \mathbb{Q}_p = F_p \cap M(\mathbb{Z}_p)u_p = F_p \cap M(\mathbb{Z}_p)u$$

for all primes p , it follows that $I = F \cap M(\mathbb{Z})u$, so $u \in U_I$. We have proven that Φ_I is surjective.

For the proof of injectivity, suppose that $u, v \in U_I$ are such that $\Phi_I(u) = \Phi_I(v)$. The assumption that $u, v \in U_I$ means that there is an isomorphism of \mathcal{O} -modules $F \cap M(\mathbb{Z})u \cong F \cap M(\mathbb{Z})v$. As we saw above this implies that there exists $x \in F^\times$ such that $F \cap M(\mathbb{Z})u = F \cap M(\mathbb{Z})vx$. Replacing v with vx it follows that

$$\hat{F} \cap M(\hat{\mathbb{Z}})\hat{u} = \hat{F} \cap M(\hat{\mathbb{Z}})\hat{v}. \quad (11)$$

The assumption that $\Phi_I(u) = \Phi_I(v)$ means that there exist $\tilde{z} \in M(\hat{\mathbb{Z}})^\times$ and $\tilde{x} \in \hat{F}^\times$ such that $\hat{u} = \tilde{z}\hat{v}\tilde{x}$. Together with (11) this implies that

$$\hat{F} \cap M(\hat{\mathbb{Z}})\hat{v} = \hat{F} \cap M(\hat{\mathbb{Z}})\hat{v}\tilde{x}$$

and hence $\tilde{x} \in \hat{v}^{-1}M(\hat{\mathbb{Z}})^\times \hat{v}$. In other words, there exists $\tilde{y} \in M(\hat{\mathbb{Z}})^\times$ such that $\hat{v}\tilde{x} = \tilde{y}\hat{v}$. We deduce that

$$\hat{u} = \tilde{z}\hat{v}\tilde{x} = (\tilde{z}\tilde{y})\hat{v}.$$

Replacing \tilde{z} with $\tilde{z}\tilde{y} \in M(\hat{\mathbb{Z}})^\times$, we now have that

$$\tilde{z} = \hat{u}\hat{v}^{-1} \in M(\hat{\mathbb{Z}})^\times \cap M(\mathbb{Q})^\times = M(\mathbb{Z})^\times.$$

Writing $z = \tilde{z} \in M(\mathbb{Z})^\times$ we get that $u = zv$ and injectivity is proven. \square

In this final section we complete the proof of the Main Theorem. We do this by using our results on orders in subfields of division algebras of degree four to interpret the Prime Geodesic Theorem algebraically. This will then yield information about the class numbers of those orders.

2 Comparing Geodesics and Orders

2.1 Regular geodesics

Let F be a number field with r real embeddings and s pairs of complex conjugate embeddings and let $t = r + s - 1$. Let \mathcal{O}_F denote the ring of integers of F and \mathcal{O}_F^\times the unit group therein. By Dirichlet's unit theorem ([27], I Theorem 7.4), there exist units $\varepsilon_1, \dots, \varepsilon_t \in \mathcal{O}_F^\times$ such that every $\varepsilon \in \mathcal{O}_F^\times$ can be written uniquely as a product

$$\varepsilon = \zeta \varepsilon_1^{\nu_1} \cdots \varepsilon_t^{\nu_t},$$

where ζ is a root of unity and $\nu_i \in \mathbb{Z}$. The set $\{\varepsilon_1, \dots, \varepsilon_t\}$ is not uniquely determined. We shall refer to such a set of units as a *system of fundamental units*. If $\mathcal{O} \subset \mathcal{O}_F$ is an order of F and $\{\varepsilon_1, \dots, \varepsilon_t\}$ a system of fundamental units then there exist $\mu_i \in \mathbb{N}$ and units $\bar{\varepsilon}_i = \varepsilon_i^{\mu_i}$ such that every $\varepsilon \in \mathcal{O}^\times$ can be written uniquely as a product

$$\varepsilon = \zeta \bar{\varepsilon}_1^{\nu_1} \cdots \bar{\varepsilon}_t^{\nu_t}$$

where ζ is a root of unity and $\nu_i \in \mathbb{Z}$. Once again, the set $\{\bar{\varepsilon}_1, \dots, \bar{\varepsilon}_t\}$ is not uniquely determined. We shall call such a set of units a *system of fundamental units of \mathcal{O}* .

If $\tau_1, \dots, \tau_{t+1}$ are distinct embeddings of F into \mathbb{C} which are pairwise non-conjugate, then the *regulator* $R(\mathcal{O})$ of an order $\mathcal{O} \subset \mathcal{O}_F$ is defined as the absolute value of the determinant of an arbitrary minor of rank t of the matrix

$$(\log |\tau_i(\bar{\varepsilon}_j)|)_{ij},$$

where $1 \leq i \leq t+1$ and $1 \leq j \leq t$. The value of the regulator does not depend on the choice of a system of fundamental units.

We shall sometimes refer, somewhat imprecisely, to the elements of a system of fundamental units simply as *fundamental units*. In the case $t = 1$, let ε_1 be a fundamental unit of an order \mathcal{O} in F . We shall refer to the elements of the set $\{\zeta \varepsilon_1^{\pm 1} : \zeta \text{ root of unity in } F\}$ as *the fundamental units of \mathcal{O}* , or in the case that $\mathcal{O} = \mathcal{O}_F$ *the fundamental units of F* .

In the case that F is a totally complex quartic field we have $t = 1$, so we can choose a fundamental unit ε_1 such that for all $\varepsilon \in \mathcal{O}_F^\times$ we have $\varepsilon = \zeta \varepsilon_1^{\nu_1}$, where ζ is a root of unity and $\nu_1 \in \mathbb{Z}$. Then ε_1 is determined up to inversion and multiplication by a root of unity. In this case the regulator of an order $\mathcal{O} \subset \mathcal{O}_F$ of F with fundamental unit $\bar{\varepsilon}_1$ satisfies

$$R(\mathcal{O}) = |\log |\tau(\bar{\varepsilon}_1)||,$$

where τ is any embedding of F into \mathbb{C} .

We consider subfields of the field F . Apart from \mathbb{Q} these are all quadratic. By Dirichlet's unit theorem, real quadratic fields contain a single fundamental unit (up to inversion and multiplication by ± 1) and complex quadratic fields contain no fundamental unit. We can see then that F can have at most one real subfield. Let $C^r(S)$ and $C^c(S)$ be respectively the subsets of $C(S)$ consisting of fields with and without a real quadratic subfield. Let $O^r(S)$ and $O^c(S)$ be respectively the subsets of $O(S)$ consisting of orders in fields in $C^r(S)$ and $C^c(S)$. Then $C(S) = C^r(S) \cup C^c(S)$ and $O(S) = O^r(S) \cup O^c(S)$.

Let $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$. Then by Lemma 1.4 the centraliser $M(\mathbb{Q})_\gamma$ is a totally complex quartic field which embeds into $M(\mathbb{Q})$ and we denote this subfield of $M(\mathbb{Q})$ by F_γ . We say that an element $\gamma \in \Gamma$ is weakly neat if the adjoint $\text{Ad}(\gamma)$ has no non-trivial roots of unity as eigenvalues. Let $\mathcal{E}_P^{p,\text{rw}}(\Gamma)$ be the set of primitive, regular, weakly neat elements in $\mathcal{E}_P(\Gamma)$.

Lemma 2.1 *Let $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$. Then $F_\gamma \in C^c(S)$ if and only if $[\gamma] \in \mathcal{E}_P^{p,\text{rw}}(\Gamma)$.*

Proof: Let \mathcal{O} be the maximal order in F and let \mathcal{O}^\times denote the group of units. By Dirichlet's unit theorem we can see that F_γ contains a real quadratic subfield if and only if $\mathcal{O}^\times \cap \mathbb{R} \neq \{\pm 1\}$. Let $\gamma_1 \in \mathcal{O}^\times$ be a fundamental unit. The element γ is a unit F_γ so there exists a root of unity ζ and $n \in \mathbb{Z}$ such that $\gamma = \zeta \gamma_1^n$. If there also exist a root of unity ξ and $m \in \mathbb{Z} \setminus \{0\}$ such that $\xi \gamma_1^m \in \mathbb{R}$ then γ_1 is not weakly neat and so neither is γ .

Conversely, suppose γ is not weakly neat. We know that γ is conjugate in G to an element $a_\gamma b_\gamma \in A^- B$. From the assumption that γ is not weakly neat it follows that there exists $m \in \mathbb{N}$ such that one of the components of b_γ^m is diagonal. Since the group AB is abelian we have that γ^m is conjugate in G to $a_\gamma^m b_\gamma^m$. Since $\gamma^m \in \mathcal{E}_P(\Gamma)$ it follows from Lemma 1.4 that b_γ^m is diagonal and hence γ^m generates a real quadratic subfield of F_γ . The lemma follows. \square

Define the map

$$\theta : \mathcal{E}_P^{p,\text{rw}}(\Gamma) \rightarrow O^c(S)$$

by

$$\theta : [\gamma] \mapsto F_\gamma \cap M(\mathbb{Z}).$$

Let $\gamma, \delta \in \Gamma$. Then $F_{\delta\gamma\delta^{-1}} = \delta F_\gamma \delta^{-1}$, and since by Lemma 1.5 the group Γ is a subgroup of the multiplicative group $M(\mathbb{Z})^\times$, we can conclude that

$$F_{\delta\gamma\delta^{-1}} \cap M(\mathbb{Z}) = \delta (F_\gamma \cap M(\mathbb{Z})) \delta^{-1} \cong F_\gamma \cap M(\mathbb{Z}).$$

Hence the map is well defined.

Proposition 2.2 *The map θ is surjective.*

Proof: Let $\mathcal{O} \in \mathcal{O}^c(S)$ be an order in the field $F \in C^c(S)$. Since $\deg F = 4$, Proposition 1.2(b) implies that F is a maximal subfield of $M(\mathbb{Q})$.

Lemma 1.9 tells us that there exists an embedding $\sigma : F \rightarrow M(\mathbb{Q})$ such that

$$\mathcal{O} = \mathcal{O}_\sigma = \sigma^{-1}(\sigma(F) \cap M(\mathbb{Z})).$$

Let ε be a fundamental unit in \mathcal{O}^\times . Let γ be the image of ε under the embedding σ . The unit ε is integral in F , so $\gamma \in M(\mathbb{Z})$.

First we show that $\gamma \sim_G a_\gamma b_\gamma$ for some $a_\gamma \in A^-$, $b_\gamma \in B$. The field F has two pairs of conjugate embeddings into \mathbb{C} . Let σ_1, σ_2 be two distinct, non-conjugate embeddings of F into \mathbb{C} . The \mathbb{R} -algebra $F \otimes_{\mathbb{Q}} \mathbb{R}$ is isomorphic to the commutative \mathbb{R} -algebra $\mathbb{C} \oplus \mathbb{C}$ via the map

$$\alpha \otimes x \mapsto (x\sigma_1(\alpha), x\sigma_2(\alpha)).$$

We note that $\mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R} = F \otimes_{\mathbb{Q}} \mathbb{R}$ and we get the series of inclusions

$$\mathcal{O} \subset \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{R} = F \otimes_{\mathbb{Q}} \mathbb{R} \subset M(\mathbb{Q}) \otimes_{\mathbb{Q}} \mathbb{R} = \text{Mat}_4(\mathbb{R}) \subset \text{Mat}_4(\mathbb{C}).$$

Thus we see that γ may be considered as an element, which we will denote $\bar{\gamma}$, of a commutative subalgebra of $\text{Mat}_4(\mathbb{C})$ isomorphic to $\mathbb{C} \oplus \mathbb{C}$. The matrix $\bar{\gamma}$ has real entries and can be diagonalised in $\text{Mat}_4(\mathbb{C})$ to the matrix

$$X = \begin{pmatrix} \sigma_1(\gamma) & & & \\ & \overline{\sigma_1(\gamma)} & & \\ & & \sigma_2(\gamma) & \\ & & & \overline{\sigma_2(\gamma)} \end{pmatrix},$$

since the eigenvalues of $\bar{\gamma}$ are the roots of its minimal polynomial, ie. the values of γ under its different embeddings into \mathbb{C} . Let $a, b \in \mathbb{R}^+$; $\theta, \phi \in [-\pi, \pi]$ be such that $\sigma_1(\gamma) = ae^{i\theta}$ and $\sigma_2(\gamma) = be^{i\phi}$. Since $\gamma \in M(\mathbb{Z})$, we have $\prod_{\sigma} \sigma(\gamma) = N_{F|\mathbb{Q}}(\gamma) = \det \gamma = \pm 1$, where $N_{F|\mathbb{Q}}$ is the field norm and the product is over all embeddings σ of F into \mathbb{C} ([27], I Proposition 2.6(iii)). Hence $a^2b^2 = \pm 1$. But a and b are both real so we must have $a^2b^2 = 1$, and so $b = a^{-1}$ and we have

$$X = \begin{pmatrix} ae^{i\theta} & & & \\ & ae^{-i\theta} & & \\ & & \frac{1}{a}e^{i\phi} & \\ & & & \frac{1}{a}e^{-i\phi} \end{pmatrix}.$$

Without loss of generality we assume $a < b$ so that $a \in (0, 1)$. Let R be the 2×2 matrix

$$\frac{1}{\sqrt{2}} \begin{pmatrix} i & -1 \\ 1 & -i \end{pmatrix}$$

and Y the 4×4 matrix

$$\begin{pmatrix} R & \\ & R \end{pmatrix} \in \text{Mat}_4(\mathbb{C})$$

Then X is conjugate in $\text{Mat}_4(\mathbb{C})$ via Y to the real matrix

$$X' = \begin{pmatrix} aR(\theta) & \\ & \frac{1}{a}R(\phi) \end{pmatrix} \in A^-B.$$

So $\bar{\gamma}$ is conjugate in $\text{Mat}_4(\mathbb{C})$ to an element of A^-B , hence by [26], XIV Corollary 2.3, the matrix $\bar{\gamma}$ is conjugate in $\text{Mat}_4(\mathbb{R})$ to X' , that is $(Z')^{-1}\bar{\gamma}Z' = X'$ for some $Z' \in \text{Mat}_4(\mathbb{R})$. Since Z' is invertible we

have that $n = \det Z' \neq 0$. Let $Z = |n|^{-\frac{1}{4}} Z'$. Then $\det Z = \pm 1$ and $Z^{-1} \bar{\gamma} Z = X'$, so that γ is conjugate in $\mathrm{SL}_4^{\pm}(\mathbb{R})$ to an element of $A^- B$. Suppose that $\det Z = -1$. Let W be the matrix

$$W = \begin{pmatrix} 0 & 1 & & \\ 1 & 0 & & \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix}.$$

Then $ZW \in G$ and $(ZW)^{-1} \bar{\gamma} ZW = X''$, where

$$X'' = \begin{pmatrix} aR(-\theta) & \\ & \frac{1}{a}R(\phi) \end{pmatrix} \in A^- B.$$

Hence γ is conjugate in G to an element of $A^- B$.

We also saw above that $\det \gamma = 1$ and so $\gamma \in \Gamma$ and hence $\gamma \in \mathcal{E}_P(\Gamma)$. It then follows from Lemma 1.4 that γ , and hence also ε , generates either a real quadratic or a totally complex quartic field over \mathbb{Q} . The field generated by ε over \mathbb{Q} is a subfield of F . However $F \in C^c(S)$ so has no real quadratic subfields. Hence $\mathbb{Q}(\gamma) \cong \mathbb{Q}(\varepsilon)$ is a totally complex quartic field and Lemma 1.4 tells us that γ is regular. It then follows from Lemma 2.1 that γ is weakly neat.

It remains to show that γ is primitive in Γ . Note that $\mathbb{Q}(\varepsilon)$ is a quartic field contained in and hence equal to the field F . Recall that we write $F_{\gamma} = M(\mathbb{Q})_{\gamma}$ for the centraliser of γ in $M(\mathbb{Q})$. Then we have that $F_{\gamma} = \mathbb{Q}(\gamma) \cong F$ and $\mathcal{O}^{\times} \cong F_{\gamma} \cap M(\mathbb{Z})^{\times}$. The fundamental unit ε is primitive in \mathcal{O}^{\times} and so $\gamma = \sigma(\varepsilon)$ is primitive in $F_{\gamma} \cap M(\mathbb{Z})^{\times}$. Suppose γ is not primitive in Γ . Then there exists $\gamma_0 \in \Gamma \subset M(\mathbb{Z})^{\times}$ such that $\gamma = \gamma_0^{\kappa}$ for some $\kappa \in \mathbb{N}$. However we also have $\gamma_0 \in F_{\gamma}$ and so $\gamma_0 \in F_{\gamma} \cap M(\mathbb{Z})^{\times}$, which is a contradiction. Hence γ is primitive in Γ and we have $\gamma \in \mathcal{E}_P^{\mathrm{reg}}(\Gamma)$.

This concludes the proof of the surjectivity of θ . \square

Lemma 2.3 *Let ζ be a torsion element of $M(\mathbb{Z})$. Then $\det(\zeta) = 1$.*

Proof: By Proposition 1.2(b), the element ζ generates a subfield $\mathbb{Q}(\zeta)$ of $M(\mathbb{Q})$ of degree 1, 2 or 4 over \mathbb{Q} . If $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 1$ or 2 then by Lemma 1.5 we have $\det(\zeta) = 1$.

For a primitive n^{th} root of unity ξ , the degree $[\mathbb{Q}(\xi) : \mathbb{Q}]$ is equal to $\varphi(n) = \#\{1 \leq m \leq n : (m, n) = 1\}$. From [5], Chapter II, §2 we see that

$$\varphi(n) = \prod_{i=1}^r p_i^{a_i-1} (p_i - 1),$$

where $n = p_1^{a_1} \dots p_r^{a_r}$ is the prime decomposition of n . It is then straightforward to show that $[\mathbb{Q}(\xi) : \mathbb{Q}] = 4$ if and only if $n = 5, 8, 10$ or 12 . In these cases the minimal polynomial of ξ is respectively $x^4 + x^3 + x^2 + x + 1$, $x^4 + 1$, $x^4 - x^3 + x^2 - x + 1$ or $x^4 - x^2 + 1$. In each of these cases we read off from the constant term of the minimal polynomial that $N_{\mathbb{Q}(\xi)|\mathbb{Q}}(\xi) = 1$. The lemma follows. \square

For $\mathcal{O} \in O(S)$ let $\mu_{\mathcal{O}}$ be the number of roots of unity in the order \mathcal{O} . For $[\gamma] \in \mathcal{E}_P^{\mathrm{reg}}(\Gamma)$ let μ_{γ} denote the number of roots of unity in the order $F_{\gamma} \cap M(\mathbb{Z})$. Note that $F_{\gamma} \cap M(\mathbb{Z})$ is equal to the centraliser $M(\mathbb{Z})_{\gamma}$ of γ in $M(\mathbb{Z})$, and by Lemma 2.3 the roots of unity in $M(\mathbb{Z})_{\gamma}$ are all in Γ and hence in Γ_{γ} . It follows that μ_{γ} is equal to the cardinality of the torsion part of Γ_{γ} . It is also immediate from the definitions that, writing $\mathcal{O}_{\gamma} = F_{\gamma} \cap M(\mathbb{Z})$, we have $\mu_{\gamma} = \mu_{\mathcal{O}_{\gamma}}$.

Lemma 2.4 *Let $\mathcal{O} \in O(S)$ be an order in the field $F \in C(S)$ and let $f(x)$ be the minimal polynomial over \mathbb{Q} of a fundamental unit in \mathcal{O} . Then the number of roots of $f(x)$ in F which are also fundamental units in \mathcal{O} is independent of the choice of fundamental unit. We call this number $\kappa(\mathcal{O})$. Note that $\kappa(\mathcal{O})$ is equal to 1, 2 or 4.*

Proof: Let ε be a fundamental unit in \mathcal{O} with minimal polynomial $f(x)$ over \mathbb{Q} . Suppose there exists another fundamental unit $\delta \in \mathcal{O}^{\times}$ with $\delta \neq \varepsilon$ which is also a root of $f(x)$. Then there exist embeddings α and β of F into \mathbb{C} such that $\alpha(\varepsilon) = \beta(\delta)$.

Let $\eta \in \mathcal{O}^{\times}$ also be a fundamental unit in \mathcal{O} with minimal polynomial $g(x)$ over \mathbb{Q} . Then $\eta = \zeta \varepsilon^{\pm 1}$ for some root of unity $\zeta \in \mathcal{O}^{\times}$. We have

$$\alpha(\eta) = \alpha(\zeta \varepsilon^{\pm 1}) = \alpha(\zeta) \alpha(\varepsilon)^{\pm 1} = \alpha(\zeta) \beta(\delta)^{\pm 1}.$$

Let n be the order of the root of unity ζ . The order \mathcal{O} is a ring so contains all roots of unity of order n and hence there exists an n^{th} root of unity $\xi \in \mathcal{O}^{\times}$ such that $\beta(\xi) = \alpha(\zeta)$. Let θ be the fundamental unit $\xi \delta^{\pm 1} \in \mathcal{O}^{\times}$. Then $\alpha(\eta) = \beta(\theta)$ and so θ is also a root of $g(x)$. The lemma follows. \square

Proposition 2.5 *The map θ is $\frac{4h(\mathcal{O})\lambda_S(\mathcal{O})\mu_{\mathcal{O}}}{\kappa(\mathcal{O})}$ to one.*

Proof: The question is, given $\mathcal{O} \in O(S)$, how many conjugacy classes $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$ are there such that $F_\gamma \cap M(\mathbb{Z}) \cong \mathcal{O}$. Suppose \mathcal{O} is an order in the field F . We saw in the proof of the previous proposition that given an embedding $\sigma : F \hookrightarrow M(\mathbb{Q})$ such that $\mathcal{O}_\sigma = \mathcal{O}$ and a fundamental unit $\varepsilon \in \mathcal{O}^\times$ the element $\gamma = \sigma(\varepsilon)$ satisfies both $F_\gamma \cap M(\mathbb{Z}) \cong \mathcal{O}$ and $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$. Conversely, it is clear that for $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$, the element γ is a fundamental unit in the order $F_\gamma \cap M(\mathbb{Z})$.

Recall that $M(\mathbb{Z})^\times$ acts on the set $\Sigma(\mathcal{O})$ from the left and that, by Proposition 1.10, the cardinality of the set $M(\mathbb{Z})^\times \backslash \Sigma(\mathcal{O})$ is $h(\mathcal{O})\lambda_S(\mathcal{O})$. If $\varepsilon, \delta \in \mathcal{O}^\times$ are fundamental units and σ, τ are embeddings of F into $M(\mathbb{Q})$ such that $\mathcal{O}_\sigma = \mathcal{O}_\tau = \mathcal{O}$, then $\sigma(\varepsilon)$ and $\tau(\delta)$ are in the same $M(\mathbb{Z})^\times$ -conjugacy class if and only if there exists an automorphism α of F such that $\alpha(\delta) = \varepsilon$ and the embeddings σ and $\tau \circ \alpha$ are in the same class modulo $M(\mathbb{Z})^\times$.

We will show that for each $\gamma \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$ the $M(\mathbb{Z})^\times$ -conjugacy class of γ decomposes into two Γ -conjugacy classes. If $\gamma, \delta \in \Gamma$ are in the same $M(\mathbb{Z})^\times$ -conjugacy class we shall write $[[\gamma]] = [[\delta]]$. For $\gamma \in \Gamma$, if γ is central in $M(\mathbb{Q})$ then clearly the conjugacy class $[[\gamma]] = \{\gamma\}$. Conversely, if $[[\gamma]] = \{\gamma\}$ then γ commutes with every element of $M(\mathbb{Z})$ and, since $M(\mathbb{Z})$ is an order in $M(\mathbb{Q})$, it follows that γ commutes with every element of $M(\mathbb{Q})$. Hence the conjugacy class $[[\gamma]]$ consists of a single element if and only if γ is central in $M(\mathbb{Q})$. Note that, by [31], Theorem 34.9, the image of $M(\mathbb{Z})$ under the map \det is equal to \mathbb{Z} , so there exist elements of $M(\mathbb{Z})$ whose image under \det is -1 .

Let $\gamma \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$. Then γ is not central in $M(\mathbb{Q})$ so there exists $\delta \neq \gamma$ in $[[\gamma]]$ such that $\gamma = \eta^{-1}\delta\eta$ for some $\eta \in M(\mathbb{Z})^\times$ with $\det(\eta) = -1$. Suppose further that $[\gamma] = [\delta]$, so that $\gamma = \theta^{-1}\delta\theta$ for some $\theta \in \Gamma$. Then $\gamma = \eta^{-1}\theta\gamma\theta^{-1}\eta$, so $\xi = \eta^{-1}\theta$ is an element of F_γ with $\det(\xi) = -1$. By Lemma 1.5 we then have $\xi \in F_\gamma \cap M(\mathbb{Z})^\times$, where $\mathcal{O} = F_\gamma \cap M(\mathbb{Z})$ is an order in the totally complex quartic field F_γ and $\mathcal{O}^\times = F_\gamma \cap M(\mathbb{Z})^\times$ is the group of units. But since F_γ is totally complex quartic, Lemma 1.5 tells us that $\det(\xi) = 1$ and hence, by contradiction, $[\gamma] \neq [\delta]$. This shows that each $M(\mathbb{Z})^\times$ -conjugacy class of elements in $\mathcal{E}_P^{p,\text{reg}}(\Gamma)$ decomposes into at least two Γ -conjugacy classes.

Suppose that $[[\gamma]] = [[\delta]]$ but $[\gamma] \neq [\delta]$. Then there exists $\eta \in M(\mathbb{Z})^\times$ such that $\gamma = \eta^{-1}\delta\eta$ and $\det(\eta) = -1$. Let $\beta \in \Gamma$ also be such that $[[\gamma]] = [[\beta]]$ but $[\gamma] \neq [\beta]$. Then there exists $\theta \in M(\mathbb{Z})^\times$ such that $\gamma = \theta^{-1}\beta\theta$ and $\det(\theta) = -1$. Then $\delta = \eta\theta^{-1}\beta\theta\eta^{-1}$, where $\det(\theta\eta^{-1}) = 1$ so $[\delta] = [\beta]$. Hence each $M(\mathbb{Z})^\times$ -conjugacy class of elements in $\mathcal{E}_P^{p,\text{reg}}(\Gamma)$ decomposes into precisely two Γ -conjugacy classes.

We conclude that the choice of a fundamental unit $\varepsilon \in \mathcal{O}^\times$ gives us $2h(\mathcal{O})\lambda_S(\mathcal{O})$ Γ -conjugacy classes $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$ such that $F_\gamma \cap M(\mathbb{Z}) \cong \mathcal{O}$. We have seen that the choice of fundamental unit is determined up to inversion and multiplication by a root of unity so there are $2\mu_{\mathcal{O}}$ choices for ε . We saw in the previous proposition that for a given embedding σ of F into $M(\mathbb{Q})$ and choice of a fundamental unit $\varepsilon \in \mathcal{O}$ there is a conjugacy class $[\gamma_{\sigma,\varepsilon}] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$ with $\sigma(\varepsilon) = \gamma_{\sigma,\varepsilon}$. However, we saw above that if there exists an automorphism α of F such that $\delta = \alpha(\varepsilon)$, then setting $\tau = \sigma \circ \alpha^{-1}$ we have $[\gamma_{\sigma,\varepsilon}] = [\gamma_{\tau,\delta}]$. Such an automorphism exists if and only if δ is a root of the minimal polynomial of ε over \mathbb{Q} . The claim of the proposition follows. \square

Lemma 2.6 *Let $\gamma \in \mathcal{E}_P^{p,\text{rw}}(\Gamma)$ so that γ is conjugate in G to $a_\gamma b_\gamma \in A^- B$ where*

$$a_\gamma = \begin{pmatrix} a & & & \\ & a & & \\ & & a^{-1} & \\ & & & a^{-1} \end{pmatrix} \quad \text{and} \quad b_\gamma = \begin{pmatrix} R(\theta) & & & \\ & R(\phi) & & \\ & & & \\ & & & \end{pmatrix}$$

for some $a \in (0, 1)$, $\theta, \phi \in \mathbb{R}$. If $\kappa(\mathcal{O}_\gamma) > 1$ then either $\theta + \phi$ or $\theta - \phi$ is in $\frac{\pi}{2}\mathbb{Z} \cup \frac{\pi}{3}\mathbb{Z}$.

Proof: The element γ is a fundamental unit in \mathcal{O}_γ . We shall write $f(x)$ for its minimal polynomial. The roots of $f(x)$ are the eigenvalues of γ , which are $\alpha_1 = ae^{i\theta}$, $\alpha_2 = ae^{-i\theta}$, $\alpha_3 = a^{-1}e^{i\phi}$, $\alpha_4 = a^{-1}e^{-i\phi}$.

Suppose $\kappa(\mathcal{O}_\gamma) > 1$. Then there exist $i, j \in \{1, 2, 3, 4\}$, $i \neq j$ and a root of unity ζ such that $\alpha_i = \zeta\alpha_j^{\pm 1}$. If $\alpha_i = \zeta\alpha_j$ then $\alpha_i\alpha_j^{-1} = \zeta$ and either $\{i, j\} = \{1, 2\}$ or $\{i, j\} = \{3, 4\}$. Without loss of generality take $i = 1$ and $j = 2$, then $\zeta = \alpha_1\alpha_2^{-1} = e^{i2\theta}$. It follows that if $n \in \mathbb{N}$ is such that $\zeta^n = 1$ then $\alpha_1^{2n} = a^n \in (0, 1)$ and so F_γ has a real quadratic subfield. However, by Lemma 2.1 this contradicts the assumption that $\gamma \in \mathcal{E}_P^{p,\text{rw}}(\Gamma)$, so we must have $\alpha_i = \zeta\alpha_j^{-1}$.

By considering the possible values of i and j which would satisfy $\alpha_i = \zeta\alpha_j^{-1}$ we see that either $\theta + \phi$ or $\theta - \phi$ is equal to $q\pi$, where $q \in \mathbb{Q}$ is such that $\zeta = e^{iq\pi}$. It remains to show what the possible values for q are, that is, which roots of unity may occur in \mathcal{O}_γ . We saw in the proof of Lemma 2.3 that the only roots of unity which may occur in a quartic field are ± 1 and roots of order 3, 4, 5, 6, 8, 10 or 12. If ζ is a root of order 5, 8, 10 or 12 then ζ generates a totally complex quartic field, however, $\mathbb{Q}(\zeta)$ has the real

quadratic subfield $\mathbb{Q}(\zeta + \zeta^{-1})$, which possibility is excluded in our case. So we are left with the possibility that $\zeta = \pm 1$ or ζ is a root of order 3, 4 or 6, which implies the claim of the lemma. \square

Lemma 2.7 *Let $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$. Then*

$$\chi_1(\Gamma_\gamma) = \frac{1}{\mu_\gamma}.$$

Proof: By Proposition 1.10 of [13],

$$\chi_1(\Gamma_\gamma) = \frac{[\Gamma_{\gamma,A} : \Gamma'_{\gamma,A}]}{[\Gamma_\gamma : \Gamma'_\gamma]},$$

where $\Gamma' \subset \Gamma$ is a torsion free subgroup of finite index. In the case under consideration we have that Γ_γ is isomorphic as a group to the group of norm one elements in the order $\mathcal{O}_\gamma = F_\gamma \cap M(\mathbb{Z})$. By Lemma 1.5 this is equal to the group of units $\mathcal{O}_\gamma^\times$. By Dirichlet's unit theorem and Lemma 2.3 it follows that

$$\Gamma_\gamma \cong \varepsilon^\mathbb{Z} \times \mu(\gamma),$$

for some generator ε and where $\mu(\gamma)$ is the finite cyclic group of roots of unity in $\mathcal{O}_\gamma^\times$. It then follows that

$$\Gamma'_\gamma \cong \varepsilon^{k\mathbb{Z}},$$

for some $k \in \mathbb{N}$. Since every torsion element in Γ_γ is sent to the identity under the projection onto $\Gamma_{\gamma,A}$ we also have the isomorphisms

$$\Gamma_{\gamma,A} \cong \varepsilon^\mathbb{Z}$$

and

$$\Gamma'_{\gamma,A} \cong \varepsilon^{k\mathbb{Z}}.$$

The lemma follows. \square

Let $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$. Then γ is conjugate in G to a matrix $a_\gamma b_\gamma$, where $a_\gamma = \text{diag}(a, a, a^{-1}, a^{-1})$ for some $0 < a < 1$ and

$$b_\gamma = \begin{pmatrix} R(\theta) & \\ & R(\phi) \end{pmatrix}$$

for some θ, ϕ . Recall that the length l_γ of γ is defined to be $8|\log a|$ and $N(\gamma) = e^{l_\gamma}$. For $\mathcal{O} \in \mathcal{O}(S)$ let $\varepsilon_\mathcal{O}$ be a fundamental unit of \mathcal{O} and $R(\mathcal{O}) = 2|\log |\varepsilon_\mathcal{O}||$ the regulator of \mathcal{O} and let $r(\mathcal{O}) = e^{4R(\mathcal{O})}$. Under the map θ , the element γ corresponds to a fundamental unit of the order $\theta([\gamma])$ and it is clear that

$$r(\theta([\gamma])) = N(\gamma).$$

We recall from the proof of Lemma 1.4 that $\theta([\gamma])$ is an order in the field $\mathbb{Q}(ae^{i\theta}, a^{-1}e^{i\phi})$. By Lemma 2.10 of [13] we have that $\text{tr } \tilde{\sigma}(\gamma) = 4(1 - \cos 2\theta)(1 - \cos 2\phi)$. Let

$$\nu(\gamma) = \prod_{\alpha} \left(1 - \frac{\alpha(\gamma)}{|\alpha(\gamma)|} \right),$$

where the product is over the embeddings of F_γ into \mathbb{C} . A simple calculation then shows that

$$\text{tr } \tilde{\sigma}(\gamma) = (1 - e^{i\theta})(1 - e^{-i\theta})(1 - e^{i\phi})(1 - e^{-i\phi}) = \nu(\gamma).$$

We summarise the results of this section in the following:

Proposition 2.8 *The map θ is surjective and $\frac{4h(\mathcal{O})\lambda_S(\mathcal{O})\mu_\mathcal{O}}{\kappa(\mathcal{O})}$ to one. For $[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma)$ we have that $\chi_1(\Gamma_\gamma) = 1/\mu_\gamma$, that $\text{tr } \tilde{\sigma}(\gamma) = \nu(\gamma)$ and that $N(\gamma) = r(\theta([\gamma]))$.*

2.2 Class numbers of orders in totally complex quartic fields

We are now in a position to prove our main theorem.

Theorem 2.9 (Main Theorem) *Let S be a finite, non-empty set of prime numbers with an even number of elements. For $x > 0$ let*

$$\pi_S(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S) \\ R(\mathcal{O}) \leq x}} \lambda_S(\mathcal{O}) h(\mathcal{O}),$$

Then, as $x \rightarrow \infty$ we have

$$\pi_S(x) \sim \frac{e^{4x}}{8x}.$$

Proof: By [1], Proposition 17.6 we know that Γ has a weakly neat subgroup Γ' which is of finite index. Hence there exists $n_\Gamma \in \mathbb{N}$ such that all roots of unity which are eigenvalues of $\text{Ad}(\gamma)$ for some $\gamma \in \Gamma$ have order less than or equal to n_Γ . Define the sets

$$B_1^0 = \left\{ \begin{pmatrix} R(\theta) & \\ & R(\phi) \end{pmatrix} \in B : \theta, \phi \notin \pi\mathbb{Z} \cup \frac{\pi}{2}\mathbb{Z} \cup \dots \cup \frac{\pi}{n_\Gamma}\mathbb{Z} \right\}$$

and

$$B_2^0 = B_1^0 \cup \left\{ \begin{pmatrix} R(\theta) & \\ & R(\phi) \end{pmatrix} \in B : (\theta + \phi), (\theta - \phi) \notin \frac{\pi}{2}\mathbb{Z} \cup \frac{\pi}{3}\mathbb{Z} \right\}.$$

For $x > 0$ define the functions

$$\pi_1^{\text{rw}}(x) = \sum_{\substack{[\gamma] \in \mathcal{E}_P^{P, \text{rw}}(\Gamma) \\ N(\gamma) \leq x}} \chi_1(\Gamma_\gamma) \quad \text{and} \quad \pi_2^{\text{rw}}(x) = \sum_{\substack{[\gamma] \in \mathcal{E}_P^{P, \text{rw}}(\Gamma); \kappa(\mathcal{O}_\gamma)=1 \\ N(\gamma) \leq x}} \chi_1(\Gamma_\gamma).$$

Setting $B^0 = B_1^0$ in Theorem 3.2 of [13] we get as $x \rightarrow \infty$

$$\pi_1^{\text{rw}}(x) \sim \frac{2x}{\log x}. \quad (12)$$

Setting $B^0 = B_2^0$ in Theorem 3.2 of [13] we get, using Lemma 2.6, as $x \rightarrow \infty$

$$\pi_2^{\text{rw}}(x) \sim \frac{2x}{\log x}. \quad (13)$$

We also define the following functions for $x > 0$:

$$\pi_{S,1}(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S) \\ R(\mathcal{O}) \leq x}} \frac{\lambda_S(\mathcal{O})}{\kappa(\mathcal{O})} h(\mathcal{O}) \quad \text{and} \quad \pi_{S,2}(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S); \kappa(\mathcal{O}_\gamma)=1 \\ R(\mathcal{O}) \leq x}} \lambda_S(\mathcal{O}) h(\mathcal{O}).$$

By Proposition 2.8 and the fact that $N(\gamma) = e^{4R(\mathcal{O}_\gamma)}$ we deduce from (12) that

$$\pi_{S,1}(x) \sim \frac{e^{4x}}{8x} \quad (14)$$

and from (13) that

$$\pi_{S,2}(x) \sim \frac{e^{4x}}{8x}. \quad (15)$$

For $x > 0$ define

$$\pi'_{S,2}(x) = \pi_{S,1}(x) - \pi_{S,2}(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S); \kappa(\mathcal{O}_\gamma) > 1 \\ R(\mathcal{O}) \leq x}} \frac{\lambda_S(\mathcal{O})}{\kappa(\mathcal{O})} h(\mathcal{O}).$$

Then from (14) and (15) it follows that

$$\pi'_{S,2}(x) = o\left(\frac{e^{4x}}{x}\right).$$

Since $\kappa(\mathcal{O}) \leq 4$ for all $\mathcal{O} \in \mathcal{O}^c(S)$ we have

$$\pi_{S,2}(x) \leq \pi_S(x) \leq \pi_{S,2}(x) + 4\pi'_{S,2}(x)$$

and the theorem follows. \square

We can also prove the following:

Theorem 2.10 *Let S be a finite, non-empty set of prime numbers with an even number of elements. For $x > 0$ let*

$$\tilde{\pi}_S(x) = \sum_{\substack{\mathcal{O} \in \mathcal{O}^c(S) \\ R(\mathcal{O}) \leq x}} \nu(\mathcal{O}) \lambda_S(\mathcal{O}) h(\mathcal{O}),$$

where

$$\nu(\mathcal{O}) = \frac{1}{2\mu_{\mathcal{O}}} \sum_{\varepsilon} \prod_{\alpha} \left(1 - \frac{\alpha(\varepsilon)}{|\alpha(\varepsilon)|}\right),$$

where the sum is over the $2\mu_{\mathcal{O}}$ different fundamental units of \mathcal{O} and the product is over the embeddings of \mathcal{O} into \mathbb{C} .

Then, as $x \rightarrow \infty$ we have

$$\pi_S(x) \sim \frac{e^{4x}}{2x}.$$

Proof: Let $\mathcal{E}_P^{p,\text{rnw}}(\Gamma) = \mathcal{E}_P^{p,\text{reg}}(\Gamma) \setminus \mathcal{E}_P^{p,\text{rw}}(\Gamma)$ be the set of regular, non weakly neat elements in $\mathcal{E}_P^p(\Gamma)$. Setting $B^0 = B^{\text{reg}}$ in Theorem 3.2 of [13] we get

$$\sum_{\substack{[\gamma] \in \mathcal{E}_P^{p,\text{reg}}(\Gamma) \\ N(\gamma) \leq x}} \chi_1(\Gamma_{\gamma}) \sim \frac{2x}{\log x}$$

and with (12) above it follows that

$$\sum_{\substack{[\gamma] \in \mathcal{E}_P^{p,\text{rnw}}(\Gamma) \\ N(\gamma) \leq x}} \chi_1(\Gamma_{\gamma}) = o\left(\frac{x}{\log x}\right).$$

It follows from Lemma 2.10 of [13] that $0 \leq \text{tr } \tilde{\sigma}(b_{\gamma}) \leq 16$ for all $\gamma \in \mathcal{E}_P(\Gamma)$, and hence we have

$$\sum_{\substack{[\gamma] \in \mathcal{E}_P^{p,\text{rnw}}(\Gamma) \\ N(\gamma) \leq x}} \chi_1(\Gamma_{\gamma}) \text{tr } \tilde{\sigma}(b_{\gamma}) = o\left(\frac{x}{\log x}\right).$$

It then follows from Theorem 3.1 of [13] that

$$\sum_{\substack{[\gamma] \in \mathcal{E}_P^{p,\text{rw}}(\Gamma) \\ N(\gamma) \leq x}} \chi_1(\Gamma_{\gamma}) \text{tr } \tilde{\sigma}(b_{\gamma}) \sim \frac{8x}{\log x}.$$

We can also deduce from (12) and (13) that

$$\sum_{\substack{[\gamma] \in \mathcal{E}_P^{p,\text{rw}}(\Gamma); \kappa(\mathcal{O}_{\gamma}) > 1 \\ N(\gamma) \leq x}} \chi_1(\Gamma_{\gamma}) \text{tr } \tilde{\sigma}(b_{\gamma}) = o\left(\frac{x}{\log x}\right).$$

The theorem then follows from Proposition 2.8 using the same arguments as in the proof of the previous theorem. \square

The methods we have used to deduce the asymptotic result for class numbers from the Prime Geodesic Theorem were not sharp enough to preserve the error term which was proven there. However, we make the following conjecture:

Conjecture 2.11 *Under the conditions of Theorem 2.9, as $x \rightarrow \infty$ we have*

$$\pi_S(x) = \frac{1}{2} L(4x) + O\left(\frac{e^{3x}}{x}\right),$$

where

$$L(x) = \int_1^x \frac{e^t}{t} dt.$$

References

- [1] **Borel, A.:** *Introduction aux groupes arithmétiques*. Hermann, Paris 1969.
- [2] **Borel, A.; Harder, G.:** *Existence of discrete cocompact subgroups of reductive groups over local fields*. J. Reine Angew. Math. 298, 53-64(1978).
- [3] **Borel, A.; Wallach, N.:** *Continuous Cohomology, Discrete Groups, and Representations of Reductive Groups*. Ann. Math. Stud. 94, Princeton 1980.
- [4] **Cartan, H.; Eilenberg, S.:** *Homological algebra*. Princeton University Press, Princeton, N. J., 1956.
- [5] **Chandrasekharan, K.:** *Introduction to Analytic Number Theory*. Springer-Verlag 1968.
- [6] **Conway, J.:** *Functions of one complex variable*. Springer-Verlag, New York, 1978.
- [7] **Deitmar, A.:** *Higher torsion zeta functions*. Adv. Math. 110, 109-128 (1995).
- [8] **Deitmar, A.:** *Geometric zeta-functions of locally symmetric spaces*. American Journal of Mathematics. 122, vol 5, 887-926 (2000).
- [9] **Deitmar, A.:** *Class numbers of orders in cubic fields*. J. Number Theory 95, 150-166 (2002).
- [10] **Deitmar, A.:** *A prime geodesic theorem for higher rank spaces*. Geometric and Functional Analysis 14, 1238-1266 (2004).
- [11] **Deitmar, A.:** *A prime geodesic theorem for higher rank spaces*. Geometric and Functional Analysis 14, 1238-1266 (2004).
- [12] **Deitmar, A.; Hoffman, J.:** *The Ihara-Selberg zeta function for PGL_3 and Hecke operators*. International Journal of Mathematics (2005).
- [13] **Deitmar, A.; Pavey, M.:** *A prime geodesic theorem for SL_4* . math.DG/0605048
- [14] **Duistermaat, J.J.; Kolk, J.A.C.; Varadarajan, V.S.:** *Spectra of locally symmetric manifolds of negative curvature*. Invent. math. 52 (1979) 27-93.
- [15] **Gauss, C. F.:** *Disquisitiones arithmeticae* Springer-Verlag, New York, 1986.
- [16] **Gelfand, I.M.; Graev, M.I.; Pyatetskii-Shapiro, I.I.:** *Representation Theory and Automorphic Functions*. Saunders 1969.
- [17] **Hardy, G. H.; Riesz, M.:** *The general theory of Dirichlet's series*. Cambridge Tracts in Mathematics and Mathematical Physics, No.18, Stechert-Hafner, Inc., New York, 1964.
- [18] **Harish-Chandra:** *Harmonic analysis on real reductive groups I. The theory of the constant term*. J. Func. Anal. 19, 104-204 (1975).
- [19] **Hecht, H.; Schmid, W.:** *Characters, asymptotics and \mathfrak{n} -homology of Harish-Chandra modules*. Acta Math. 151, 49-151 (1983).
- [20] **Hochschild, G.; Serre, J.-P.:** *Cohomology of Lie algebras*. Ann. of Math. 57, 591-603 (1953).
- [21] **Hochschild, G.; Serre, J.-P.:** *Cohomology of group extensions*. Trans. Amer. Math. Soc. 74, 110-134 (1953)
- [22] **Hopf, H.; Samelson, H.:** *Ein Satz über die Wirkungsräume geschlossener Liescher Gruppen*. Comment. Math. Helv. 13, 240-251 (1941).
- [23] **Howe, R.; Moore, C.:** *Asymptotic properties of unitary representations*. J. Funct. Anal. 32, 72-96 (1979).
- [24] **Knapp, A.:** *Representation Theory of Semisimple Lie Groups*. Princeton University Press 1986.
- [25] **Kneser, M.:** *Strong Approximation*. Proc. Symp. Pure Math. 9, 187-196 (1967).

- [26] **Lang, S.:** *Algebra*. Revised third edition. Graduate Texts in Mathematics, 211. Springer-Verlag, New York, 2002.
- [27] **Neukirch, J.:** *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften. 322. Berlin: Springer 1999.
- [28] **Pierce, R. S.:** *Associative algebras*. Springer-Verlag, New York-Berlin, 1982.
- [29] **Randol, B.:** *On the asymptotic distribution of closed geodesics on compact Riemann surfaces*. Trans. AMS 233, 241-247 (1977).
- [30] **Randol, B.:** *The Riemann hypothesis for Selberg's zeta-function and the asymptotic behavior of eigenvalues of the Laplace operator*. Trans. Amer. Math. Soc. 236, 209-223 (1978).
- [31] **Reiner, I.:** *Maximal Orders*. Academic Press 1975.
- [32] **Sarnak, P.:** *Class Numbers of Indefinite Binary Quadratic Forms*. J. Number Theory 15, 229-247 (1982).
- [33] **Selberg, A.:** *Harmonic Analysis and Discontinuous Groups in weakly symmetric Riemannian spaces with Applications to Dirichlet Series*. J. Indian. Math. Soc. 20, 47-87 (1956).
- [34] **Siegel, C.L.:** *The average measure of quadratic forms with given determinant and signature*. Ann. of Math. 45, 667-685 (1944).
- [35] **Speh, B.:** *The unitary dual of $Gl(3, R)$ and $Gl(4, R)$* . Math. Ann. 258, 113-133 (1981).
- [36] **Wallach, N.:** *On the Selberg Trace Formula in the case of compact quotient*. Bull. AMS 82 No 2, 171-195 (1976).
- [37] **Warner, F.:** *Foundations of differentiable manifolds and Lie groups*. Springer-Verlag, New York 1983.
- [38] **Wolf, J.:** *Discrete groups, symmetric spaces, and global holonomy*. Amer. J. Math. 84, 527-542 (1962).